INTERNET LAW (Law 793)
COURSE READER

Professor Eric Goldman
Fall 2010

Last updated July 25, 2010

Editing Notes:

- Textual omissions are noted with ellipses
- Omitted footnotes are not indicated, but all footnote numbers are original
- In-text citations are omitted without indication (including parathentical explanations and some parallel citations)
- Although I have tried to preserve the original formatting (such as italics, bold and blockquotes), some of this formatting may have changed or been lost in the conversion.

To improve readability, I have aggressively stripped out case citations and parenthetical explanations (more so than in most casebooks). If you are interested in the court's actual words or intend to quote or cite one of these opinions, I STRONGLY recommend that you pull the actual opinion and read the unedited version first.

American Civil Liberties Union v. Reno, 929 F. Supp. 824 (E.D. Pa. 1996)
Per curiam

[Editor's note: per Congress' request, litigation against the Communications Decency Act proceeded to a three judge district court panel. This excerpt is Section II of that court's decision, the Findings of Fact. The litigants stipulated to the first 48 paragraphs of these factual findings, and the remainder was issued per curiam.]

…The Nature of Cyberspace
The Creation of the Internet and the Development of Cyberspace

1. The Internet is not a physical or tangible entity, but rather a giant network which interconnects innumerable smaller groups of linked computer networks. It is thus a network of networks. This is best understood if one considers what a linked group of computers—referred to here as a "network"—is, and what it does. Small networks are now ubiquitous (and are often called "local area networks"). For example, in many United States Courthouses, computers are linked to each other for the purpose of exchanging files and messages (and to share equipment such as printers). These are networks.

2. Some networks are "closed" networks, not linked to other computers or networks. Many networks, however, are connected to other networks, which are in turn connected to other networks in a manner which permits each computer in any network to communicate with computers on any other network in the system. This global Web of linked networks and computers is referred to as the Internet.

3. The nature of the Internet is such that it is very difficult, if not impossible, to determine its size at a given moment. It is indisputable, however, that the Internet has experienced extraordinary growth in recent years. In 1981, fewer than 300 computers were linked to the Internet, and by 1989, the number stood at fewer than 90,000 computers. By 1993, over 1,000,000 computers were linked. Today, over 9,400,000 host computers worldwide, of which approximately 60 percent located within the United States, are estimated to be linked to the Internet. This count does not include the personal computers people use to access the Internet using modems. In all, reasonable estimates are that as many as 40 million people around the world can and do access the enormously flexible communication Internet medium. That figure is expected to grow to 200 million Internet users by the year 1999.

4. Some of the computers and computer networks that make up the Internet are owned by governmental and public institutions, some are owned by non-profit organizations, and some are privately owned. The resulting whole is a decentralized, global medium of communications—or "cyberspace"—that links people, institutions, corporations, and governments around the world. The Internet is an international system. This communications medium allows any of the literally tens of millions of people with access to the Internet to exchange information. These communications can occur almost instantaneously, and can be directed either to specific individuals, to a broader group of people interested in a particular subject, or to the world as a whole.

5. The Internet had its origins in 1969 as an experimental project of the Advanced Research Project Agency ("ARPA"), and was called ARPANET. This network linked computers and computer networks owned by the military, defense contractors, and university laboratories conducting defense-related research. The network later allowed researchers across the country to access directly and to use extremely powerful supercomputers located at a few key universities and laboratories. As it evolved far beyond its research origins in the United States to encompass universities, corporations, and people around the world, the ARPANET came to be called the "DARPA Internet," and finally just the "Internet."

6. From its inception, the network was designed to be a decentralized, self-maintaining series of redundant links between computers and computer networks, capable of rapidly transmitting communications without direct human involvement or control, and with the automatic ability to re-route communications if one or more individual links were damaged or otherwise unavailable. Among other goals, this redundant system of linked computers was designed to allow vital research and communications to continue even if portions of the network were damaged, say, in a war.

7. To achieve this resilient nationwide (and ultimately global) communications medium, the ARPANET encouraged the creation of multiple links to and from each computer (or computer network) on the network. Thus, a computer located in Washington, D.C., might be linked (usually using dedicated telephone lines) to other computers in neighboring states or on the Eastern seaboard. Each of those computers could in turn be linked to other computers, which themselves would be linked to other computers.

8. A communication sent over this redundant series of linked computers could travel any of a number of routes to its destination. Thus, a message sent from a computer in Washington, D.C., to a computer in Palo Alto, California, might first be sent to a computer in Philadelphia, and then be forwarded to a computer in Pittsburgh, and then to Chicago, Denver, and Salt Lake City, before finally reaching Palo Alto. If the message could not travel along that path (because of military attack, simple technical malfunction, or other reason), the message would automatically (without human intervention or even knowledge) be re-routed, perhaps, from Washington, D.C. to Richmond, and then to Atlanta, New Orleans, Dallas, Albuquerque, Los Angeles, and finally to Palo Alto. This type of transmission, and re-routing, would likely occur in a matter of seconds.

9. Messages between computers on the Internet do not necessarily travel entirely along the same path. The Internet uses "packet switching" communication protocols that allow individual messages to be subdivided into smaller "packets" that are then sent independently to the destination, and are then automatically reassembled by the receiving computer. While all packets of a given message often travel along the same path to the destination, if computers along the route become overloaded, then packets can be re-routed to less loaded computers.

10. At the same time that ARPANET was maturing (it subsequently ceased to exist), similar networks developed to link universities, research facilities, businesses, and individuals around the world. These other formal or loose networks included BITNET, CSNET, FIDONET, and USENET. Eventually, each of these networks (many of which overlapped) were themselves linked together, allowing users of any computers linked to any one of the networks to transmit

communications to users of computers on other networks. It is this series of linked networks (themselves linking computers and computer networks) that is today commonly known as the Internet.

11. No single entity—academic, corporate, governmental, or non-profit—administers the Internet. It exists and functions as a result of the fact that hundreds of thousands of separate operators of computers and computer networks independently decided to use common data transfer protocols to exchange communications and information with other computers (which in turn exchange communications and information with still other computers). There is no centralized storage location, control point, or communications channel for the Internet, and it would not be technically feasible for a single entity to control all of the information conveyed on the Internet.

How Individuals Access the Internet

12. Individuals have a wide variety of avenues to access cyberspace in general, and the Internet in particular. In terms of physical access, there are two common methods to establish an actual link to the Internet. First, one can use a computer or computer terminal that is directly (and usually permanently) connected to a computer network that is itself directly or indirectly connected to the Internet. Second, one can use a "personal computer" with a "modem" to connect over a telephone line to a larger computer or computer network that is itself directly or indirectly connected to the Internet. As detailed below, both direct and modem connections are made available to people by a wide variety of academic, governmental, or commercial entities.

13. Students, faculty, researchers, and others affiliated with the vast majority of colleges and universities in the United States can access the Internet through their educational institutions. Such access is often via direct connection using computers located in campus libraries, offices, or computer centers, or may be through telephone access using a modem from a student's or professor's campus or off-campus location. Some colleges and universities install "ports" or outlets for direct network connections in each dormitory room or provide access via computers located in common areas in dormitories. Such access enables students and professors to use information and content provided by the college or university itself, and to use the vast amount of research resources and other information available on the Internet worldwide.

14. Similarly, Internet resources and access are sufficiently important to many corporations and other employers that those employers link their office computer networks to the Internet and provide employees with direct or modem access to the office network (and thus to the Internet). Such access might be used by, for example, a corporation involved in scientific or medical research or manufacturing to enable corporate employees to exchange information and ideas with academic researchers in their fields.

15. Those who lack access to the Internet through their schools or employers still have a variety of ways they can access the Internet. Many communities across the country have established "free-nets" or community networks to provide their citizens with a local link to the Internet (and to provide local-oriented content and discussion groups). The first such community network, the Cleveland Free-Net Community Computer System, was established in 1986, and free-nets now

exist in scores of communities as diverse as Richmond, Virginia, Tallahassee, Florida, Seattle, Washington, and San Diego, California. Individuals typically can access free-nets at little or no cost via modem connection or by using computers available in community buildings. Free-nets are often operated by a local library, educational institution, or non-profit community group.

16. Individuals can also access the Internet through many local libraries. Libraries often offer patrons use of computers that are linked to the Internet. In addition, some libraries offer telephone modem access to the libraries' computers, which are themselves connected to the Internet. Increasingly, patrons now use library services and resources without ever physically entering the library itself. Libraries typically provide such direct or modem access at no cost to the individual user.

17. Individuals can also access the Internet by patronizing an increasing number of storefront "computer coffee shops," where customers—while they drink their coffee—can use computers provided by the shop to access the Internet. Such Internet access is typically provided by the shop for a small hourly fee.

18. Individuals can also access the Internet through commercial and non-commercial "Internet service providers" that typically offer modem telephone access to a computer or computer network linked to the Internet. Many such providers—including the members of plaintiff Commercial Internet Exchange Association—are commercial entities offering Internet access for a monthly or hourly fee. Some Internet service providers, however, are non-profit organizations that offer free or very low cost access to the Internet. For example, the International Internet Association offers free modem access to the Internet upon request. Also, a number of trade or other non-profit associations offer Internet access as a service to members.

19. Another common way for individuals to access the Internet is through one of the major national commercial "online services" such as America Online, CompuServe, the Microsoft Network, or Prodigy. These online services offer nationwide computer networks (so that subscribers can dial-in to a local telephone number), and the services provide extensive and well organized content within their own proprietary computer networks. In addition to allowing access to the extensive content available within each online service, the services also allow subscribers to link to the much larger resources of the Internet. Full access to the online service (including access to the Internet) can be obtained for modest monthly or hourly fees. The major commercial online services have almost twelve million individual subscribers across the United States.

20. In addition to using the national commercial online services, individuals can also access the Internet using some (but not all) of the thousands of local dial-in computer services, often called "bulletin board systems" or "BBSs." With an investment of as little as $2,000.00 and the cost of a telephone line, individuals, non-profit organizations, advocacy groups, and businesses can offer their own dial-in computer "bulletin board" service where friends, members, subscribers, or customers can exchange ideas and information. BBSs range from single computers with only one telephone line into the computer (allowing only one user at a time), to single computers with many telephone lines into the computer (allowing multiple simultaneous users), to multiple linked computers each servicing multiple dial-in telephone lines (allowing multiple simultaneous

users). Some (but not all) of these BBS systems offer direct or indirect links to the Internet. Some BBS systems charge users a nominal fee for access, while many others are free to the individual users.

21. Although commercial access to the Internet is growing rapidly, many users of the Internet—such as college students and staff—do not individually pay for access (except to the extent, for example, that the cost of computer services is a component of college tuition). These and other Internet users can access the Internet without paying for such access with a credit card or other form of payment.

Methods to Communicate Over the Internet

22. Once one has access to the Internet, there are a wide variety of different methods of communication and information exchange over the network. These many methods of communication and information retrieval are constantly evolving and are therefore difficult to categorize concisely. The most common methods of communications on the Internet (as well as within the major online services) can be roughly grouped into six categories:

(1) one-to-one messaging (such as “e-mail”),

(2) one-to-many messaging (such as “listserv”),

(3) distributed message databases (such as “USENET newsgroups”),

(4) real time communication (such as “Internet Relay Chat”),

(5) real time remote computer utilization (such as “telnet”), and

(6) remote information retrieval (such as “ftp,” “gopher,” and the “World Wide Web”).

Most of these methods of communication can be used to transmit text, data, computer programs, sound, visual images (i.e., pictures), and moving video images.

23. One-to-one messaging. One method of communication on the Internet is via electronic mail, or “e-mail,” comparable in principle to sending a first class letter. One can address and transmit a message to one or more other people. E-mail on the Internet is not routed through a central control point, and can take many and varying paths to the recipients. Unlike postal mail, simple e-mail generally is not “sealed” or secure, and can be accessed or viewed on intermediate computers between the sender and recipient (unless the message is encrypted).

24. One-to-many messaging. The Internet also contains automatic mailing list services (such as “listservs”), [also referred to by witnesses as “mail exploders”] that allow communications about particular subjects of interest to a group of people. For example, people can subscribe to a “listserv” mailing list on a particular topic of interest to them. The subscriber can submit messages on the topic to the listserv that are forwarded (via e-mail), either automatically or through a human moderator overseeing the listserv, to anyone who has subscribed to the mailing

list. A recipient of such a message can reply to the message and have the reply also distributed to everyone on the mailing list. This service provides the capability to keep abreast of developments or events in a particular subject area. Most listserv-type mailing lists automatically forward all incoming messages to all mailing list subscribers. There are thousands of such mailing list services on the Internet, collectively with hundreds of thousands of subscribers. Users of "open" listservs typically can add or remove their names from the mailing list automatically, with no direct human involvement. Listservs may also be "closed," i.e., only allowing for one's acceptance into the listserv by a human moderator.

25. Distributed message databases. Similar in function to listservs—but quite different in how communications are transmitted—are distributed message databases such as "USENET newsgroups." User-sponsored newsgroups are among the most popular and widespread applications of Internet services, and cover all imaginable topics of interest to users. Like listservs, newsgroups are open discussions and exchanges on particular topics. Users, however, need not subscribe to the discussion mailing list in advance, but can instead access the database at any time. Some USENET newsgroups are "moderated" but most are open access. For the moderated newsgroups, all messages to the newsgroup are forwarded to one person who can screen them for relevance to the topics under discussion. USENET newsgroups are disseminated using ad hoc, peer to peer connections between approximately 200,000 computers (called USENET "servers") around the world. For unmoderated newsgroups, when an individual user with access to a USENET server posts a message to a newsgroup, the message is automatically forwarded to all adjacent USENET servers that furnish access to the newsgroup, and it is then propagated to the servers adjacent to those servers, etc. The messages are temporarily stored on each receiving server, where they are available for review and response by individual users. The messages are automatically and periodically purged from each system after a time to make room for new messages. Responses to messages, like the original messages, are automatically distributed to all other computers receiving the newsgroup or forwarded to a moderator in the case of a moderated newsgroup. The dissemination of messages to USENET servers around the world is an automated process that does not require direct human intervention or review.

26. There are newsgroups on more than fifteen thousand different subjects. In 1994, approximately 70,000 messages were posted to newsgroups each day, and those messages were distributed to the approximately 190,000 computers or computer networks that participate in the USENET newsgroup system. Once the messages reach the approximately 190,000 receiving computers or computer networks, they are available to individual users of those computers or computer networks. Collectively, almost 100,000 new messages (or "articles") are posted to newsgroups each day.

27. Real time communication. In addition to transmitting messages that can be later read or accessed, individuals on the Internet can engage in an immediate dialog, in "real time", with other people on the Internet. In its simplest forms, "talk" allows one-to-one communications and "Internet Relay Chat" (or IRC) allows two or more to type messages to each other that almost immediately appear on the others' computer screens. IRC is analogous to a telephone party line, using a computer and keyboard rather than a telephone. With IRC, however, at any one time there are thousands of different party lines available, in which collectively tens of thousands of users are engaging in conversations on a huge range of subjects. Moreover, one can create a new

party line to discuss a different topic at any time. Some IRC conversations are “moderated” or include “channel operators.”

28. In addition, commercial online services such as America Online, CompuServe, the Microsoft Network, and Prodigy have their own “chat” systems allowing their members to converse.

29. Real time remote computer utilization. Another method to use information on the Internet is to access and control remote computers in “real time” using “telnet.” For example, using telnet, a researcher at a university would be able to use the computing power of a supercomputer located at a different university. A student can use telnet to connect to a remote library to access the library’s online card catalog program.

30. Remote information retrieval. The final major category of communication may be the most well known use of the Internet-the search for and retrieval of information located on remote computers. There are three primary methods to locate and retrieve information on the Internet.

31. A simple method uses “ftp” (or file transfer protocol) to list the names of computer files available on a remote computer, and to transfer one or more of those files to an individual’s local computer.

32. Another approach uses a program and format named “gopher” to guide an individual’s search through the resources available on a remote computer.

The World Wide Web

33. A third approach, and fast becoming the most well-known on the Internet, is the “World Wide Web.” The Web utilizes a “hypertext” formatting language called hypertext markup language (HTML), and programs that “browse” the Web can display HTML documents containing text, images, sound, animation and moving video. Any HTML document can include links to other types of information or resources, so that while viewing an HTML document that, for example, describes resources available on the Internet, one can “click” using a computer mouse on the description of the resource and be immediately connected to the resource itself. Such “hyperlinks” allow information to be accessed and organized in very flexible ways, and allow people to locate and efficiently view related information even if the information is stored on numerous computers all around the world.

34. Purpose. The World Wide Web (W3C) was created to serve as the platform for a global, online store of knowledge, containing information from a diversity of sources and accessible to Internet users around the world. Though information on the Web is contained in individual computers, the fact that each of these computers is connected to the Internet through W3C protocols allows all of the information to become part of a single body of knowledge. It is currently the most advanced information system developed on the Internet, and embraces within its data model most information in previous networked information systems such as ftp, gopher, wais, and Usenet.

35. History. W3C was originally developed at CERN, the European Particle Physics Laboratory, and was initially used to allow information sharing within internationally dispersed teams of researchers and engineers. Originally aimed at the High Energy Physics community, it has spread to other areas and attracted much interest in user support, resource recovery, and many other areas which depend on collaborative and information sharing. The Web has extended beyond the scientific and academic community to include communications by individuals, non-profit organizations, and businesses.

36. Basic Operation. The World Wide Web is a series of documents stored in different computers all over the Internet. Documents contain information stored in a variety of formats, including text, still images, sounds, and video. An essential element of the Web is that any document has an address (rather like a telephone number). Most Web documents contain "links." These are short sections of text or image which refer to another document. Typically the linked text is blue or underlined when displayed, and when selected by the user, the referenced document is automatically displayed, wherever in the world it actually is stored. Links for example are used to lead from overview documents to more detailed documents, from tables of contents to particular pages, but also as cross-references, footnotes, and new forms of information structure.

37. Many organizations now have "home pages" on the Web. These are documents which provide a set of links designed to represent the organization, and through links from the home page, guide the user directly or indirectly to information about or relevant to that organization.

38. As an example of the use of links, if these Findings were to be put on a World Wide Web site, its home page might contain links such as those:

* THE NATURE OF CYBERSPACE
* CREATION OF THE INTERNET AND THE DEVELOPMENT OF CYBERSPACE
* HOW PEOPLE ACCESS THE INTERNET
* METHODS TO COMMUNICATE OVER THE INTERNET

39. Each of these links takes the user of the site from the beginning of the Findings to the appropriate section within this Adjudication. Links may also take the user from the original Web site to another Web site on another computer connected to the Internet. These links from one computer to another, from one document to another across the Internet, are what unify the Web into a single body of knowledge, and what makes the Web unique. The Web was designed with a maximum target time to follow a link of one tenth of a second.

40. Publishing. The World Wide Web exists fundamentally as a platform through which people and organizations can communicate through shared information. When information is made available, it is said to be "published" on the Web. Publishing on the Web simply requires that the "publisher" has a computer connected to the Internet and that the computer is running W3C server software. The computer can be as simple as a small personal computer costing less than $1500 dollars or as complex as a multi-million dollar mainframe computer. Many Web publishers choose instead to lease disk storage space from someone else who has the necessary computer facilities, eliminating the need for actually owning any equipment oneself.

41. The Web, as a universe of network accessible information, contains a variety of documents prepared with quite varying degrees of care, from the hastily typed idea, to the professionally executed corporate profile. The power of the Web stems from the ability of a link to point to any document, regardless of its status or physical location.

42. Information to be published on the Web must also be formatted according to the rules of the Web standards. These standardized formats assure that all Web users who want to read the material will be able to view it. Web standards are sophisticated and flexible enough that they have grown to meet the publishing needs of many large corporations, banks, brokerage houses, newspapers and magazines which now publish "online" editions of their material, as well as government agencies, and even courts, which use the Web to disseminate information to the public. At the same time, Web publishing is simple enough that thousands of individual users and small community organizations are using the Web to publish their own personal "home pages," the equivalent of individualized newsletters about that person or organization, which are available to everyone on the Web.

43. Web publishers have a choice to make their Web sites open to the general pool of all Internet users, or close them, thus making the information accessible only to those with advance authorization. Many publishers choose to keep their sites open to all in order to give their information the widest potential audience. In the event that the publishers choose to maintain restrictions on access, this may be accomplished by assigning specific user names and passwords as a prerequisite to access to the site. Or, in the case of Web sites maintained for internal use of one organization, access will only be allowed from other computers within that organization's local network.

44. Searching the Web. A variety of systems have developed that allow users of the Web to search particular information among all of the public sites that are part of the Web. Services such as Yahoo, Magellan, Altavista, Webcrawler, and Lycos are all services known as "search engines" which allow users to search for Web sites that contain certain categories of information, or to search for key words. For example, a Web user looking for the text of Supreme Court opinions would type the words "Supreme Court" into a search engine, and then be presented with a list of World Wide Web sites that contain Supreme Court information. This list would actually be a series of links to those sites. Having searched out a number of sites that might contain the desired information, the user would then follow individual links, browsing through the information on each site, until the desired material is found. For many content providers on the Web, the ability to be found by these search engines is very important.

45. Common standards. The Web links together disparate information on an ever-growing number of Internet-linked computers by setting common information storage formats (HTML) and a common language for the exchange of Web documents (HTTP). Although the information itself may be in many different formats, and stored on computers which are not otherwise compatible, the basic Web standards provide a basic set of standards which allow communication and exchange of information. Despite the fact that many types of computers are used on the Web, and the fact that many of these machines are otherwise incompatible, those

who “publish” information on the Web are able to communicate with those who seek to access information with little difficulty because of these basic technical standards.

46. A distributed system with no centralized control. Running on tens of thousands of individual computers on the Internet, the Web is what is known as a distributed system. The Web was designed so that organizations with computers containing information can become part of the Web simply by attaching their computers to the Internet and running appropriate World Wide Web software. No single organization controls any membership in the Web, nor is there any single centralized point from which individual Web sites or services can be blocked from the Web. From a user’s perspective, it may appear to be a single, integrated system, but in reality it has no centralized control point.

47. Contrast to closed databases. The Web’s open, distributed, decentralized nature stands in sharp contrast to most information systems that have come before it. Private information services such as Westlaw, Lexis/Nexis, and Dialog, have contained large storehouses of knowledge, and can be accessed from the Internet with the appropriate passwords and access software. However, these databases are not linked together into a single whole, as is the World Wide Web.

48. Success of the Web in research, education, and political activities. The World Wide Web has become so popular because of its open, distributed, and easy-to-use nature. Rather than requiring those who seek information to purchase new software or hardware, and to learn a new kind of system for each new database of information they seek to access, the Web environment makes it easy for users to jump from one set of information to another. By the same token, the open nature of the Web makes it easy for publishers to reach their intended audiences without having to know in advance what kind of computer each potential reader has, and what kind of software they will be using….

72. Although parental control software currently can screen for certain suggestive words or for known sexually explicit sites, it cannot now screen for sexually explicit images unaccompanied by suggestive text unless those who configure the software are aware of the particular site.

73. Despite its limitations, currently available user-based software suggests that a reasonably effective method by which parents can prevent their children from accessing sexually explicit and other material which parents may believe is inappropriate for their children will soon be widely available.

Content on the Internet

74. The types of content now on the Internet defy easy classification. The entire card catalogue of the Carnegie Library is on-line, together with journals, journal abstracts, popular magazines, and titles of compact discs. The director of the Carnegie Library, Robert Croneberger, testified that on-line services are the emerging trend in libraries generally. Plaintiff Hotwired Ventures LLC organizes its Web site into information regarding travel, news and commentary, arts and entertainment, politics, and types of drinks. Plaintiff America Online, Inc., not only creates chat rooms for a broad variety of topics, but also allows members to create their own chat rooms to suit their own tastes. The ACLU uses an America Online chat room as an unmoderated forum for

people to debate civil liberties issues. Plaintiffs' expert, Scott Bradner, estimated that 15,000 newsgroups exist today, and he described his own interest in a newsgroup devoted solely to Formula 1 racing cars. America Online makes 15,000 bulletin boards available to its subscribers, who post between 200,000 and 250,000 messages each day. Another plaintiffs' expert, Howard Rheingold, participates in "virtual communities" that simulate social interaction. It is no exaggeration to conclude that the content on the Internet is as diverse as human thought.

75. The Internet is not exclusively, or even primarily, a means of commercial communication. Many commercial entities maintain Web sites to inform potential consumers about their goods and services, or to solicit purchases, but many other Web sites exist solely for the dissemination of non-commercial information. The other forms of Internet communication—e-mail, bulletin boards, newsgroups, and chat rooms—frequently have non-commercial goals. For the economic and technical reasons set forth in the following paragraphs, the Internet is an especially attractive means for not-for-profit entities or public interest groups to reach their desired audiences. There are examples in the parties' stipulation of some of the non-commercial uses that the Internet serves. Plaintiff Human Rights Watch, Inc., offers information on its Internet site regarding reported human rights abuses around the world. Plaintiff National Writers Union provides a forum for writers on issues of concern to them. Plaintiff Stop Prisoner Rape, Inc., posts text, graphics, and statistics regarding the incidence and prevention of rape in prisons. Plaintiff Critical Path AIDS Project, Inc., offers information on safer sex, the transmission of HIV, and the treatment of AIDS.

76. Such diversity of content on the Internet is possible because the Internet provides an easy and inexpensive way for a speaker to reach a large audience, potentially of millions. The start-up and operating costs entailed by communication on the Internet are significantly lower than those associated with use of other forms of mass communication, such as television, radio, newspapers, and magazines. This enables operation of their own Web sites not only by large companies, such as Microsoft and Time Warner, but also by small, not-for-profit groups, such as Stop Prisoner Rape and Critical Path AIDS Project. The Government's expert, Dr. Dan R. Olsen, agreed that creation of a Web site would cost between $1,000 and $15,000, with monthly operating costs depending on one's goals and the Web site's traffic. Commercial online services such as America Online allow subscribers to create Web pages free of charge. Any Internet user can communicate by posting a message to one of the thousands of newsgroups and bulletin boards or by engaging in an on-line "chat", and thereby reach an audience worldwide that shares an interest in a particular topic.

77. The ease of communication through the Internet is facilitated by the use of hypertext markup language (HTML), which allows for the creation of "hyperlinks" or "links". HTML enables a user to jump from one source to other related sources by clicking on the link. A link might take the user from Web site to Web site, or to other files within a particular Web site. Similarly, by typing a request into a search engine, a user can retrieve many different sources of content related to the search that the creators of the engine have collected.

78. Because of the technology underlying the Internet, the statutory term "content provider," which is equivalent to the traditional "speaker," may actually be a hybrid of speakers. Through the use of HTML, for example, Critical Path and Stop Prisoner Rape link their Web sites to

several related databases, and a user can immediately jump from the home pages of these organizations to the related databases simply by clicking on a link. America Online creates chat rooms for particular discussions but also allows subscribers to create their own chat rooms. Similarly, a newsgroup gathers postings on a particular topic and distributes them to the newsgroup's subscribers. Users of the Carnegie Library can read on-line versions of Vanity Fair and Playboy, and America Online's subscribers can peruse the New York Times, Boating, and other periodicals. Critical Path, Stop Prisoner Rape, America Online and the Carnegie Library all make available content of other speakers over whom they have little or no editorial control.

79. Because of the different forms of Internet communication, a user of the Internet may speak or listen interchangeably, blurring the distinction between "speakers" and "listeners" on the Internet. Chat rooms, e-mail, and newsgroups are interactive forms of communication, providing the user with the opportunity both to speak and to listen.

80. It follows that unlike traditional media, the barriers to entry as a speaker on the Internet do not differ significantly from the barriers to entry as a listener. Once one has entered cyberspace, one may engage in the dialogue that occurs there. In the argot of the medium, the receiver can and does become the content provider, and vice-versa.

81. The Internet is therefore a unique and wholly new medium of worldwide human communication.

Sexually Explicit Material On the Internet

82. The parties agree that sexually explicit material exists on the Internet. Such material includes text, pictures, and chat, and includes bulletin boards, newsgroups, and the other forms of Internet communication, and extends from the modestly titillating to the hardest-core.

83. There is no evidence that sexually-oriented material is the primary type of content on this new medium. Purveyors of such material take advantage of the same ease of access available to all users of the Internet, including establishment of a Web site.

84. Sexually explicit material is created, named, and posted in the same manner as material that is not sexually explicit. It is possible that a search engine can accidentally retrieve material of a sexual nature through an imprecise search, as demonstrated at the hearing. Imprecise searches may also retrieve irrelevant material that is not of a sexual nature. The accidental retrieval of sexually explicit material is one manifestation of the larger phenomenon of irrelevant search results.

85. Once a provider posts content on the Internet, it is available to all other Internet users worldwide. Similarly, once a user posts a message to a newsgroup or bulletin board, that message becomes available to all subscribers to that newsgroup or bulletin board. For example, when the UCR/California Museum of Photography posts to its Web site nudes by Edward Weston and Robert Mapplethorpe to announce that its new exhibit will travel to Baltimore and New York City, those images are available not only in Los Angeles, Baltimore, and New York City, but also in Cincinnati, Mobile, or Beijing-wherever Internet users live. Similarly, the safer

sex instructions that Critical Path posts to its Web site, written in street language so that the teenage receiver can understand them, are available not just in Philadelphia, but also in Provo and Prague. A chat room organized by the ACLU to discuss the United States Supreme Court's decision in FCC v. Pacifica Foundation would transmit George Carlin's seven dirty words to anyone who enters. Messages posted to a newsgroup dedicated to the Oklahoma City bombing travel to all subscribers to that newsgroup.

86. Once a provider posts its content on the Internet, it cannot prevent that content from entering any community. Unlike the newspaper, broadcast station, or cable system, Internet technology necessarily gives a speaker a potential worldwide audience. Because the Internet is a network of networks (as described above in Findings 1 through 4), any network connected to the Internet has the capacity to send and receive information to any other network. Hotwired Ventures, for example, cannot prevent its materials on mixology from entering communities that have no interest in that topic.

87. Demonstrations at the preliminary injunction hearings showed that it takes several steps to enter cyberspace. At the most fundamental level, a user must have access to a computer with the ability to reach the Internet (typically by way of a modem). A user must then direct the computer to connect with the access provider, enter a password, and enter the appropriate commands to find particular data. On the World Wide Web, a user must normally use a search engine or enter an appropriate address. Similarly, accessing newsgroups, bulletin boards, and chat rooms requires several steps.

88. Communications over the Internet do not "invade" an individual's home or appear on one's computer screen unbidden. Users seldom encounter content "by accident." A document's title or a description of the document will usually appear before the document itself takes the step needed to view it, and in many cases the user will receive detailed information about a site's content before he or she need take the step to access the document. Almost all sexually explicit images are preceded by warnings as to the content. Even the Government's witness, Agent Howard Schmidt, Director of the Air Force Office of Special Investigation, testified that the "odds are slim" that a user would come across a sexually explicit site by accident.

89. Evidence adduced at the hearing showed significant differences between Internet communications and communications received by radio or television. Although content on the Internet is just a few clicks of a mouse away from the user, the receipt of information on the Internet requires a series of affirmative steps more deliberate and directed than merely turning a dial. A child requires some sophistication and some ability to read to retrieve material and thereby to use the Internet unattended.

Obstacles to Age Verification on the Internet

90. There is no effective way to determine the identity or the age of a user who is accessing material through e-mail, mail exploders, newsgroups or chat rooms. An e-mail address provides no authoritative information about the addressee, who may use an e-mail "alias" or an anonymous remailer. There is also no universal or reliable listing of e-mail addresses and corresponding names or telephone numbers, and any such listing would be or rapidly become

incomplete. For these reasons, there is no reliable way in many instances for a sender to know if the e-mail recipient is an adult or a minor. The difficulty of e-mail age verification is compounded for mail exploders such as listservs, which automatically send information to all e-mail addresses on a sender's list. Government expert Dr. Olsen agreed that no current technology could give a speaker assurance that only adults were listed in a particular mail exploder's mailing list.

91. Because of similar technological difficulties, individuals posting a message to a newsgroup or engaging in chat room discussions cannot ensure that all readers are adults, and Dr. Olsen agreed. Although some newsgroups are moderated, the moderator's control is limited to what is posted and the moderator cannot control who receives the messages.

92. The Government offered no evidence that there is a reliable way to ensure that recipients and participants in such fora can be screened for age. The Government presented no evidence demonstrating the feasibility of its suggestion that chat rooms, newsgroups and other fora that contain material deemed indecent could be effectively segregated to "adult" or "moderated" areas of cyberspace.

93. Even if it were technologically feasible to block minors' access to newsgroups and similar fora, there is no method by which the creators of newsgroups which contain discussions of art, politics or any other subject that could potentially elicit "indecent" contributions could limit the blocking of access by minors to such "indecent" material and still allow them access to the remaining content, even if the overwhelming majority of that content was not indecent.

94. Likewise, participants in MUDs (Multi-User Dungeons) and MUSEs (Multi-User Simulation Environments) do not know whether the other participants are adults or minors. Although MUDs and MUSEs require a password for permanent participants, they need not give their real name nor verify their age, and there is no current technology to enable the administrator of these fantasy worlds to know if the participant is an adult or a minor.

95. Unlike other forms of communication on the Internet, there is technology by which an operator of a World Wide Web server may interrogate a user of a Web site. An HTML document can include a fill-in-the-blank "form" to request information from a visitor to a Web site, and this information can be transmitted back to the Web server and be processed by a computer program, usually a Common Gateway Interface (cgi) script. The Web server could then grant or deny access to the information sought. The cgi script is the means by which a Web site can process a fill-in form and thereby screen visitors by requesting a credit card number or adult password.

96. Content providers who publish on the World Wide Web via one of the large commercial online services, such as America Online or CompuServe, could not use an online age verification system that requires cgi script because the server software of these online services available to subscribers cannot process cgi scripts. There is no method currently available for Web page publishers who lack access to cgi scripts to screen recipients online for age.

The Practicalities of the Proffered Defenses

Note: The Government contends the CDA makes available three potential defenses to all content providers on the Internet: credit card verification, adult verification by password or adult identification number, and "tagging".

Credit Card Verification

97. Verification of a credit card number over the Internet is not now technically possible. Witnesses testified that neither Visa nor Mastercard considers the Internet to be sufficiently secure under the current technology to process transactions in that manner. Although users can and do purchase products over the Internet by transmitting their credit card number, the seller must then process the transaction with Visa or Mastercard off-line using phone lines in the traditional way. There was testimony by several witnesses that Visa and Mastercard are in the process of developing means of credit card verification over the Internet.

98. Verification by credit card, if and when operational, will remain economically and practically unavailable for many of the non-commercial plaintiffs in these actions. The Government's expert "suspect[ed]" that verification agencies would decline to process a card unless it accompanied a commercial transaction. There was no evidence to the contrary.

99. There was evidence that the fee charged by verification agencies to process a card, whether for a purchase or not, will preclude use of the credit-card verification defense by many non-profit, non-commercial Web sites, and there was no evidence to the contrary. Plaintiffs' witness Patricia Nell Warren, an author whose free Web site allows users to purchase gay and lesbian literature, testified that she must pay $1 per verification to a verification agency. Her Web site can absorb this cost because it arises in connection with the sale of books available there.

100. Using credit card possession as a surrogate for age, and requiring use of a credit card to enter a site, would impose a significant economic cost on non-commercial entities. Critical Path, for example, received 3,300 hits daily from February 4 through March 4, 1996. If Critical Path must pay a fee every time a user initially enters its site, then, to provide free access to its non-commercial site, it would incur a monthly cost far beyond its modest resources. The ACLU's Barry Steinhardt testified that maintenance of a credit card verification system for all visitors to the ACLU's Web site would require it to shut down its Web site because the projected cost would exceed its budget.

101. Credit card verification would significantly delay the retrieval of information on the Internet. Dr. Olsen, the expert testifying for the Government, agreed that even "a minute is [an] absolutely unreasonable [delay] ... [P]eople will not put up with a minute." Plaintiffs' expert Donna Hoffman similarly testified that excessive delay disrupts the "flow" on the Internet and stifles both "hedonistic" and "goal-directed" browsing.

102. Imposition of a credit card requirement would completely bar adults who do not have a credit card and lack the resources to obtain one from accessing any blocked material. At this time, credit card verification is effectively unavailable to a substantial number of Internet content providers as a potential defense to the CDA.

Adult Verification by Password

103. The Government offered very limited evidence regarding the operation of existing age verification systems, and the evidence offered was not based on personal knowledge. AdultCheck and Verify, existing systems which appear to be used for accessing commercial pornographic sites, charge users for their services. Dr. Olsen admitted that his knowledge of these services was derived primarily from reading the advertisements on their Web pages. He had not interviewed any employees of these entities, had not personally used these systems, had no idea how many people are registered with them, and could not testify to the reliability of their attempt at age verification.

104. At least some, if not almost all, non-commercial organizations, such as the ACLU, Stop Prisoner Rape or Critical Path AIDS Project, regard charging listeners to access their speech as contrary to their goals of making their materials available to a wide audience free of charge.

105. It would not be feasible for many non-commercial organizations to design their own adult access code screening systems because the administrative burden of creating and maintaining a screening system and the ongoing costs involved is beyond their reach. There was testimony that the costs would be prohibitive even for a commercial entity such as HotWired, the online version of Wired magazine.

106. There is evidence suggesting that adult users, particularly casual Web browsers, would be discouraged from retrieving information that required use of a credit card or password. Andrew Anker testified that HotWired has received many complaints from its members about HotWired's registration system, which requires only that a member supply a name, e-mail address and self-created password. There is concern by commercial content providers that age verification requirements would decrease advertising and revenue because advertisers depend on a demonstration that the sites are widely available and frequently visited.

107. Even if credit card verification or adult password verification were implemented, the Government presented no testimony as to how such systems could ensure that the user of the password or credit card is in fact over 18. The burdens imposed by credit card verification and adult password verification systems make them effectively unavailable to a substantial number of Internet content providers.

The Government's "Tagging" Proposal

108. The feasibility and effectiveness of "tagging" to restrict children from accessing "indecent" speech, as proposed by the Government has not been established. "Tagging" would require content providers to label all of their "indecent" or "patently offensive" material by imbedding a string of characters, such as "XXX," in either the URL or HTML. If a user could install software on his or her computer to recognize the "XXX" tag, the user could screen out any content with that tag. Dr. Olsen proposed a "-L18" tag, an idea he developed for this hearing in response to Mr. Bradner's earlier testimony that certain tagging would not be feasible.

109. The parties appear to agree that it is technologically feasible-"trivial", in the words of plaintiffs' expert-to imbed tags in URLs and HTML, and the technology of tagging underlies both plaintiffs' PICS proposal and the Government's "-L18" proposal.

110. The Government's tagging proposal would require all content providers that post arguably "indecent" material to review all of their online content, a task that would be extremely burdensome for organizations that provide large amounts of material online which cannot afford to pay a large staff to review all of that material. The Carnegie Library would be required to hire numerous additional employees to review its online files at an extremely high cost to its limited budget. The cost and effort would be substantial for the Library and frequently prohibitive for others. Witness Kiroshi Kuromiya testified that it would be impossible for his organization, Critical Path, to review all of its material because it has only one full and one part-time employee.

111. The task of screening and tagging cannot be done simply by using software which screens for certain words, as Dr. Olsen acknowledged, and we find that determinations as to what is indecent require human judgment.

112. In lieu of reviewing each file individually, a content provider could tag its entire site but this would prevent minors from accessing much material that is not "indecent" under the CDA.

113. To be effective, a scheme such as the -L18 proposal would require a worldwide consensus among speakers to use the same tag to label "indecent" material. There is currently no such consensus, and no Internet speaker currently labels its speech with the -L18 code or with any other widely-recognized label.

114. Tagging also assumes the existence of software that recognizes the tags and takes appropriate action when it notes tagged speech. Neither commercial Web browsers nor user-based screening software is currently configured to block a -L18 code. Until such software exists, all speech on the Internet will continue to travel to whomever requests it, without hindrance. Labelling speech has no effect in itself on the transmission (or not) of that speech. Neither plaintiffs nor the Government suggest that tagging alone would shield minors from speech or insulate a speaker from criminal liability under the CDA. It follows that all speech on any topic that is available to adults will also be available to children using the Internet (unless it is blocked by screening software running on the computer the child is using).

115. There is no way that a speaker can use current technology to know if a listener is using screening software.

116. Tags can not currently activate or deactivate themselves depending on the age or location of the receiver. Critical Path, which posts on-line safer sex instructions, would be unable to imbed tags that block its speech only in communities where it may be regarded as indecent. Critical Path, for example, must choose either to tag its site (blocking its speech in all communities) or not to tag, blocking its speech in none.

The Problems of Offshore Content and Caching

117. A large percentage, perhaps 40% or more, of content on the Internet originates outside the United States. At the hearing, a witness demonstrated how an Internet user could access a Web site of London (which presumably is on a server in England), and then link to other sites of interest in England. A user can sometimes discern from a URL that content is coming from overseas, since InterNIC allows a content provider to imbed a country code in a domain name. Foreign content is otherwise indistinguishable from domestic content (as long as it is in English), since foreign speech is created, named, and posted in the same manner as domestic speech. There is no requirement that foreign speech contain a country code in its URL. It is undisputed that some foreign speech that travels over the Internet is sexually explicit.

118. The use of "caching" makes it difficult to determine whether the material originated from foreign or domestic sources. Because of the high cost of using the trans-Atlantic and trans-Pacific cables, and because the high demand on those cables leads to bottleneck delays, content is often "cached", or temporarily stored, on servers in the United States. Material from a foreign source in Europe can travel over the trans-Atlantic cable to the receiver in the United States, and pass through a domestic caching server which then stores a copy for subsequent retrieval. This domestic caching server, rather than the original foreign server, will send the material from the cache to the subsequent receivers, without placing a demand on the trans-oceanic cables. This shortcut effectively eliminates most of the distance for both the request and the information and, hence, most of the delay. The caching server discards the stored information according to its configuration (e.g., after a certain time or as the demand for the information diminishes). Caching therefore advances core Internet values: the cheap and speedy retrieval of information.

119. Caching is not merely an international phenomenon. Domestic content providers store popular domestic material on their caching servers to avoid the delay of successive searches for the same material and to decrease the demand on their Internet connection. America Online can cache the home page of the New York Times on its servers when a subscriber first requests it, so that subsequent subscribers who make the same request will receive the same home page, but from America Online's caching service rather than from the New York Times's server.

120. Put simply, to follow the example in the prior paragraph, America Online has no control over the content that the New York Times posts to its Web site, and the New York Times has no control over America Online's distribution of that content from a caching server.

Anonymity

121. Anonymity is important to Internet users who seek to access sensitive information, such as users of the Critical Path AIDS Project's Web site, the users, particularly gay youth, of Queer Resources Directory, and users of Stop Prisoner Rape (SPR). Many members of SPR's mailing list have asked to remain anonymous due to the stigma of prisoner rape.

Plaintiffs' Choices Under the CDA

122. Many speakers who display arguably indecent content on the Internet must choose between silence and the risk of prosecution. The CDA's defenses-credit card verification, adult access

codes, and adult personal identification numbers-are effectively unavailable for non-commercial, not-for-profit entities.

123. The plaintiffs in this action are businesses, libraries, non-commercial and not-for-profit organizations, and educational societies and consortia. Although some of the material that plaintiffs post online-such as information regarding protection from AIDS, birth control or prison rape-is sexually explicit and may be considered “indecent” or “patently offensive” in some communities, none of the plaintiffs is a commercial purveyor of what is commonly termed “pornography.”

Noah v. AOL Time Warner Inc., 261 F. Supp. 2d 532 (E.D. Va. 2003)
Ellis, District Judge.

Plaintiff, on behalf of himself and a class of those similarly situated, sues his Internet service provider (ISP) for damages and injunctive relief, claiming that the ISP wrongfully refused to prevent participants in an online chat room from posting or submitting harassing comments that blasphemed and defamed plaintiff's Islamic religion and his co-religionists. Specifically, plaintiff claims his ISP's failure to prevent chat room participants from using the ISP's chat room to publish the harassing and defamatory comments constitutes a breach of the ISP's customer agreement with plaintiff and a violation of Title II of the Civil Rights Act of 1964, 42 U.S.C. § 2000a et seq.

At issue on a threshold dismissal motion are

> (i) the now familiar and well-litigated question whether a claim, like plaintiff's, which seeks to hold an ISP civilly liable as a publisher of third party statements is barred by the immunity granted ISP's by the Communications Decency Act of 1996, 47 U.S.C. § 230,
>
> (ii) the less familiar, indeed novel question whether an online chat room is a "place of public accommodation" under Title II, and
>
> (iii) the rather prosaic question whether plaintiff's breach of contract claim is barred by the very contract on which he relies, namely the Member Agreement contract.

For the reasons that follow, plaintiff's claims do not survive threshold inspection and must therefore be dismissed.

I.

Plaintiff Saad Noah, a Muslim, is a resident of Illinois and was a subscriber of defendant America Online, Inc. ("AOL")'s Internet service until he cancelled the service in July of 2000. AOL, which is located in the Eastern District of Virginia, is, according to the complaint, the world's largest Internet service provider, with more than 30 million subscribers, or "members," worldwide. Defendant AOL Time Warner Inc. is the parent company of AOL.

Among the many services AOL provides its members are what are popularly known as "chat rooms." These occur where, as AOL does here, an ISP allows its participants to use its facilities to engage in real-time electronic conversations. Chat room participants type in their comments or observations, which are then read by other chat room participants, who may then type in their responses. Conversations in a chat room unfold in real time; the submitted comments appear transiently on participants' screens and then scroll off the screen as the conversation progresses. AOL chat rooms are typically set up for the discussion of a particular topic or area of interest, and any AOL member who wishes to join a conversation in a public chat room may do so.

Two AOL chat rooms are the focus of plaintiff's claims: the "Beliefs Islam" chat room and the "Koran" chat room. It is in these chat rooms that plaintiff alleges that he and other Muslims have been harassed, insulted, threatened, ridiculed and slandered by other AOL members due to their religious beliefs. The complaint lists dozens of harassing statements made by other AOL members in these chat rooms on specified dates, all of which plaintiff alleges he brought to AOL's attention together with requests that AOL take action to enforce its member guidelines and halt promulgation of the harassing statements. The statements span a period of two and one-half years, from January 10, 1998 to July 1, 2000, and are attributable to various AOL chat room participants only by virtue of a screen name. A representative sample of the reported offensive comments follows:

> (i) On January 10, 1998 the AOL Member with the screen name "Aristotlee" wrote "islam is meaniglessssss thought," "allahsdick cut offfffffff," "dumballah bastard," "allah asssshole," "allajs dick is in holy dick place hey." "FUCK ALLAH," etc.
>
> (ii) On April 26, 1998, "Twotoneleg" wrote "I HATE MUSLIMS," "THE KORAN SUCKS," etc., and "BOSS30269" wrote "I LIKE SHOOTING MUSLIMS," "I WILL BOMB THE MIDDLE EAST," and "FUCK ISLAM."
>
> (iii) On November 4, 1998, "Hefedehefe" wrote "SMELLY TOWEL HEADS" and "MUSLIM TOWEL HEADS."
>
> (iv) On July 11, 1999, "Jzingher" wrote "The Koran and Islam are creations of Satan to distract people from the true faith which is Judaism. Mohammed was merely a huckster who found a simple people he could manipulate."
>
> (v) On July 18, 1999 "SARGON I" wrote "Qura'n lies about everything-a Satan made verses of darkness and destruction!", "Mohammed was no shit, only a killer, thief, a liar and a adulterer!", and "BYE STUPID MUSLIMS....ALL GO TO HELL."
>
> (vi) On July 1, 2000, "DXfina3000 wrote "muslims suck," "they suck ass," "korans is use to wipe ass," "fuckin muslins," and "well allah can suck my dick you peice of ass."

Plaintiff understandably complained about these offensive, obnoxious, and indecent statements, initially through the channels provided by AOL for such complaints and eventually through emails sent directly to AOL's CEO Steve Case. Plaintiff alleges that although he reported every one of the alleged violations to AOL, AOL refused to exercise its power to eliminate the harassment in the "Beliefs Islam" and "Koran" chat rooms. Moreover, plaintiff contends that AOL gave a "green light" to the harassment of Muslims in these forums, claiming that such harassment was not tolerated in chat rooms dealing with other subjects and faiths. In protest, plaintiff cancelled his AOL account in July 2000. Plaintiff further alleges that other Muslim members of AOL have also complained to AOL about similar harassing statements.

The relationship between AOL and each of its subscribing members is governed by the Terms of Service ("TOS"), which include a Member Agreement and the Community Guidelines. The Member Agreement is a "legal document that details [a member's] rights and obligations as an AOL member," and it requires, inter alia, that AOL members adhere to AOL's standards for online speech, as set forth in the Community Guidelines. These Guidelines state, in pertinent part, that

> ... You will be considered in violation of the Terms of Service if you (or others using your account) do any of the following: ....
>
> * Harass, threaten, embarrass, or do anything else to another member that is unwanted. This means: ... don't attack their race, heritage, etc....
>
> * Transmit or facilitate distribution of content that is harmful, abusive, racially or ethnically offensive, vulgar, sexually explicit, or in a reasonable person's view, objectionable. Community standards may vary, but there is no place on the service where hate speech is tolerated.
>
> * Disrupt the flow of chat in chat rooms with vulgar language, abusiveness, ...

The Member Agreement states that AOL has the right to enforce these Community Guidelines "in its sole discretion." In response to a violation, "AOL may take action against your account," ranging from "issuance of a warning about a violation to termination of your account." AOL's Community Action Team is responsible for enforcing the content and conduct standards and members are encouraged to notify AOL of violations they observe online. Importantly, however, the Member Agreement states that AOL members "... also understand and agree that the AOL Community Guidelines and the AOL Privacy Policy, including AOL's enforcement of those policies, are not intended to confer, and do not confer, any rights or remedies upon any person."

Plaintiff filed this pro se action on September 3, 2002, claiming that AOL's alleged refusal to intervene to stop the harassing statements and enforce the TOS constitutes (i) discrimination in a place of public accommodation, in violation of Title II of the Civil Rights Act of 1964, 42 U.S.C. § 2000a, and (ii) a breach of AOL's TOS and the Member Agreement. The action purports to be a class action, brought on behalf of plaintiff and all others similarly situated.

In addition to these claims raised in the complaint, plaintiff seems to assert a third claim against defendants in his response to the motion to dismiss, where he alleges new facts concerning several incidents involving disciplinary actions taken by AOL against plaintiff and other, unnamed Muslim AOL members. Although the nature of the incidents is not entirely clear, plaintiff alleges that AOL discriminated against plaintiff and other Muslim AOL members by issuing false warnings against them and terminating their accounts in an effort to silence their pro-Islam speech. Plaintiff alleges his own AOL account was briefly terminated by AOL and subsequently reinstated, but his past messages were not restored. Relying on these incidents, plaintiff belatedly claims a violation of his First Amendment rights and of the First Amendment rights of similarly situated Muslims. Although not properly pled in the complaint, given

plaintiff's pro se status this claim will nonetheless be considered on this motion to dismiss as if it had been raised in the original complaint.

Defendants AOL and AOL Time Warner filed a motion to dismiss plaintiff's claims on January 22, 2003. Nearly a month later, two days before the motion was noticed for a hearing, plaintiff belatedly requested and ultimately received, as a matter of grace, an extension of time until March 7, 2003, in which to file his response. Plaintiff missed this deadline as well, filing his response on March 10, 2003. Thereafter, defendants filed their reply on March 17, 2003. Because the issues and governing authorities are adequately set forth in the pleadings, oral argument is unnecessary and may be dispensed with, and this motion is appropriately disposed of on the papers….

IV.

Plaintiff's Title II claim fails for two alternate and independent reasons. First, plaintiff's claim against AOL is barred because of the immunity granted AOL, as an interactive computer service provider, by the Communications Decency Act of 1996, 47 U.S.C. § 230. Second, plaintiff's claim fails because a chat room is not a "place of public accommodation" as defined by Title II, 42 U.S.C. § 2000a(b). Each dismissal ground is separately addressed….

[in Section A, the court concludes that AOL is immunized by 47 U.S.C. § 230(c)(1).]

B.

Even assuming, *arguendo*, that plaintiff's Title II claim is not barred by § 230, it must nonetheless be dismissed for failure to state a claim because AOL's chat rooms and other online services do not constitute a "place of public accommodation" under Title II.

Title II provides that "[a]ll persons shall be entitled to full and equal enjoyment of the goods, services, facilities, privileges, advantages, and accommodations of any place of public accommodation, as defined in this section, without discrimination or segregation on the ground of race, color, religion, or national origin." 42 U.S.C. § 2000a(a). Title II defines a "place of public accommodation" as follows:

> Each of the following establishments which serves the public is a place of public accommodation within the meaning of this subchapter ...
>
> (1) any inn, hotel, motel, or other establishment which provides lodging to transient guests, other than an establishment located within a building which contains not more than five rooms for rent or hire and which is actually occupied by the proprietor of such establishment as his residence;
>
> (2) any restaurant, cafeteria, lunchroom, lunch counter, soda fountain, or other facility principally engaged in selling food for consumption on the premises, including, but not limited to, any such facility located on the premises of any retail establishment; or any gas station;

> (3) any motion picture house, theater, concert hall, sports arena, stadium or other place of exhibition or entertainment; and
>
> (4) any establishment (A)(i) which is physically located within the premises of any establishment otherwise covered by this subsection, or (ii) within the premises of which is physically located any such covered establishment, and (B) which holds itself out as serving patrons of such covered establishment.

42 U.S.C. § 2000a(b).

The theory of plaintiff's Title II claim is that he was denied the right of equal enjoyment of AOL's chat rooms because of AOL's alleged failure to take steps to stop the harassing comments and because of AOL's warnings to plaintiff and brief termination of plaintiff's service. In this regard, plaintiff contends that the chat rooms are "place[s] of ... entertainment" and thus within the public accommodation definition. Yet, as the relevant case law and an examination the statute's exhaustive definition make clear, "places of public accommodation" are limited to actual, physical places and structures, and thus cannot include chat rooms, which are not actual physical facilities but instead are virtual forums for communication provided by AOL to its members.

Title II's definition of "places of public accommodation" provides a list of "establishments" that qualify as such places. This list, without exception, consists of actual physical structures; namely any "inn, hotel, motel, ... restaurant, cafeteria, lunchroom, lunch counter, soda fountain, ... gasoline station ... motion picture house, theater, concert hall, sports arena [or] stadium." In addition, § 2000a(b)(4) emphasizes the importance of physical presence by referring to any "establishment ... which is physically located within" an establishment otherwise covered, or "within ... which" an otherwise covered establishment "is *physically located*." (emphasis added) Thus, in interpreting the catchall phrase "other place of exhibition or entertainment" on which plaintiff relies, the statute's consistent reference to actual physical structures points convincingly to the conclusion that the phrase does not include forums for entertainment that are not physical structures or locations.

As the Supreme Court has held, § 2000a(b)(3) should be read broadly to give effect to the statute's purpose, namely to eliminate the "daily affront and humiliation" caused by "discriminatory denials of access to *facilities* ostensibly open to the general public." (emphasis added). This broad coverage stems from a "natural reading of [the statute's] language," which should be "given full effect according to its generally accepted meaning." As such, it is clear that the reach of Title II, however broad, cannot extend beyond actual physical facilities. Given Title II's sharp focus on actual physical facilities, such as inns, motels, restaurants, gas stations, theaters, and stadiums, it is clear that Congress intended the statute to reach only the listed facilities and other similar physical structures, not to "regulate a wide spectrum of consensual human relationships."

This emphasis on actual physical facilities is reinforced by the cases rejecting Title II claims against membership organizations. In *Welsh*, the plaintiffs, who were atheists, claimed that the

Boy Scouts of America violated Title II in denying them membership, arguing that the Boy Scouts were a "place of ... entertainment." The majority of the Seventh Circuit panel in *Welsh* concluded that the Boy Scouts of America is not a "place of public accommodation" under Title II because it is not "closely connected to a particular facility." In doing so, the Welsh majority distinguished the Boy Scouts from membership organizations in which membership "functions as a 'ticket' to admission to a facility or location," that have been consistently held to be places of public accommodation under Title II. Similarly, the Ninth Circuit in *Clegg* held that the Cult Awareness Network, a nonprofit organization that provides information to the public concerning cults and supports former cult members, was not a "place of public accommodation" because it had "no affiliation with any public facility." In short, it is clear from the cases considering membership organizations that status as a place of public accommodation under Title II requires some connection to some specific physical facility or structure. As noted in *Welsh* and *Clegg*, to ignore this requirement is to ignore the plain language of the statute and to render the list of example facilities provided by the statute superfluous.

In arguing that places of public accommodation are not limited to actual physical facilities under Title II, plaintiff turns to the case law interpreting the analogous "place of public accommodation" provision under Title III of the Americans With Disability Act (ADA). While the case law concerning places of public accommodation under the ADA is more abundant than that under Title II, it is not entirely uniform. Yet, a detour into the parallel ADA cases is instructive and ultimately supports the conclusion that "places of public accommodation" must consist of, or have a clear connection to, actual physical facilities or structures.

The circuits are split regarding the essential question whether a place of public accommodation under the ADA must be an actual concrete physical structure. On the one hand, as plaintiff notes, the First Circuit has held that "places of public accommodation" under Title III of the ADA are not limited to actual physical facilities. See Carparts Distribution Center, Inc. v. Automotive Wholesaler's Assoc. of New England, Inc., 37 F.3d 12, 18-20 (1st Cir. 1994) (holding that a trade association which administers a health insurance program, without any connection to a physical facility, can be a "place of public accommodation").[9] On the other hand, the Third, Sixth and Ninth Circuits, in similar cases involving health insurance programs, followed the logic of *Welsh* and *Clegg* in holding that places of public accommodation under Title III of the ADA must be physical places. Thus, it appears that the weight of authority endorses the "actual physical structure" requirement in the ADA context as well.

Most significantly, two more recent ADA cases involving fact situations much closer to those at bar reaffirm the principle that a "places of public accommodation," even under the ADA's

[9] In reaching this conclusion, the First Circuit in *Carparts* relied on the ADA's more expansive definition of "place of public accommodation," in particular its inclusion of a "travel service," "insurance office," and "other service establishments" as places of public accommodation. Focusing on these terms, the First Circuit concluded that "Congress clearly contemplated that 'service establishments' include providers of services which do not require a person to physically enter an actual physical structure," and thus that the Title III of the ADA is not limited to "physical structures which person must enter to obtain goods and services." Simply put, the *Carparts* court found it irrational to conclude that Title III of the ADA reaches those who enter an office to purchase insurance services, but not those who purchase them over the mail or by telephone. Notably, Title II of the Civil Rights Act does not include a "travel service," "insurance office," or "other service establishments" in its definition, making the relevance of *Carparts* and its progeny to Title II questionable, at best.

broader definition, must be actual, physical facilities. In one case, the plaintiffs claimed that Southwest Airlines was in violation of the ADA because its "southwest.com" web site was incompatible with "screen reader" programs and thus inaccessible to blind persons. See Access Now, Inc. v. Southwest Airlines, Co., 227 F. Supp. 2d 1312, 1316 (S.D. Fla. 2002). Thus, the question presented was whether the airline's web site, which serves as an online ticket counter, constitutes a "place of public accommodation" under the ADA. The *Access Now* court held that places of public accommodation under the ADA are limited to "physical concrete structures," and that the web site was not an actual physical structure. Rejecting the invitation to endorse the *Carparts* approach and apply the ADA to Internet web sites despite their lack of physical presence, the *Access Now* court concluded that "[t]o expand the ADA to cover 'virtual' spaces would create new rights without well-defined standards."[11] Similarly, in another case, plaintiff contended that the defendant's digital cable system was in violation of the ADA because its on-screen channel guide was not accessible to the visually impaired. Here too, the district court rejected the notion that the digital cable system was a "place of public accommodation," because "in no way does viewing the system's images require the plaintiff to gain access to any actual physical public place," Furthermore, the *Torres* court sensibly concluded that the mere fact that the digital cable system relied on physical facilities to support and transmit its services did not convert the cable service into a "physical public place."

In sum, whether one relies on the Title II case law or looks to the broader ADA definition of public place of accommodation, it is clear that the logic of the statute and the weight of authority indicate that "places of entertainment" must be actual physical facilities. With this principle firmly established, it is clear that AOL's online chat rooms cannot be construed as "places of public accommodation" under Title II. An online chat room may arguably be a "place of entertainment," but it is not a physical structure to which a member of the public may be granted or denied access, and as such is fundamentally different from a "motion picture house, theater, concert hall, sports arena, [or] stadium." Although a chat room may serve as a virtual forum through which AOL members can meet and converse in cyberspace, it is not an "establishment," under the plain meaning of that term as defined by the statute. Unlike a theater, concert hall, arena, or any of the other "places of entertainment" specifically listed in § 2000a(b), a chat room does not exist in a particular physical location, indeed it can be accessed almost anywhere, including from homes, schools, cybercafes and libraries. In sum, although a chat room or other online forum might be referred to metaphorically as a "location" or "place," it lacks the physical presence necessary to constitute a place of public accommodation under Title II. Accordingly, even if plaintiff's Title II claim were not barred by § 230's grant of immunity to service providers, it would be fail on the independent ground that AOL's chat rooms are not places of public accommodation.

V.

Plaintiff's breach of contract claim must likewise be dismissed because the contractual rights plaintiff claims are simply not provided for in AOL's Member Agreement. The plain language of

[11] But see Doe v. Mutual of Omaha Ins. Co., 179 F.3d 557, 559 (7th Cir. 1999) (citing *Carparts* approvingly and stating, in dicta, that Title III of the ADA reaches "the owner or operator of a store, hotel, restaurant, dentist's office, travel agency, theater, *Web site*, or other facility (whether in physical space or in electronic space)") (emphasis added) (citation omitted).

the Member Agreement makes clear that AOL is not obligated to take any action against those who violate its Community Guidelines. Thus, the Member Agreement provides that AOL "has the right to enforce them *in its sole discretion*," and that "if you ... violate the AOL Community Guidelines, AOL *may* take action against your account." (emphasis added). The Member Agreement also states that "[y]ou also understand and agree that the AOL Community Guidelines and the AOL Privacy Policy, including AOL's enforcement of those policies, *are not intended to confer, and do not confer, any rights or remedies upon any person*." (emphasis added). The Member Agreement states that while AOL "reserve[s] the right to remove content that, in AOL's judgment, does not meet its standards or does not comply with AOL's current Community Guidelines ... AOL is not responsible for any failure or delay in removing such material."

In light of this plain contractual language, plaintiff cannot claim that AOL breached a duty to protect him from the harassing speech of others; the Member Agreement expressly disclaims any such duty….

Furthermore, plaintiff's attempt to cast this claim as a third-party beneficiary claim is unavailing. Under the Member Agreement, AOL no more owes a duty to other AOL members to enforce its Community Guidelines than it does with respect to plaintiff.

E.

Finally, plaintiff's belatedly-raised First Amendment claim is easily disposed of at this stage. In essence, plaintiff claims that AOL violated his First Amendment rights by issuing him warnings and briefly terminating his account, allegedly in response to his pro-Islamic statements. Yet, even assuming the truth of plaintiff's allegations, the First Amendment is of no avail to him in these circumstances; it does not protect against actions taken by private entities, rather it is "a guarantee only against abridgment by government, federal or state." Plaintiff does not argue that AOL is a state actor, nor is there any evident basis for such an argument. See Green, 318 F.3d at 472 (noting that AOL is a "private, for profit company" and rejecting the argument that AOL should be treated as a state actor); Cyber Promotions Inc. v. American Online, Inc., 948 F. Supp. 436, 441-44 (E.D. Pa. 1996) (rejecting the argument that AOL is a state actor). Accordingly, because AOL is not a state actor, plaintiff's First Amendment claim must be dismissed.

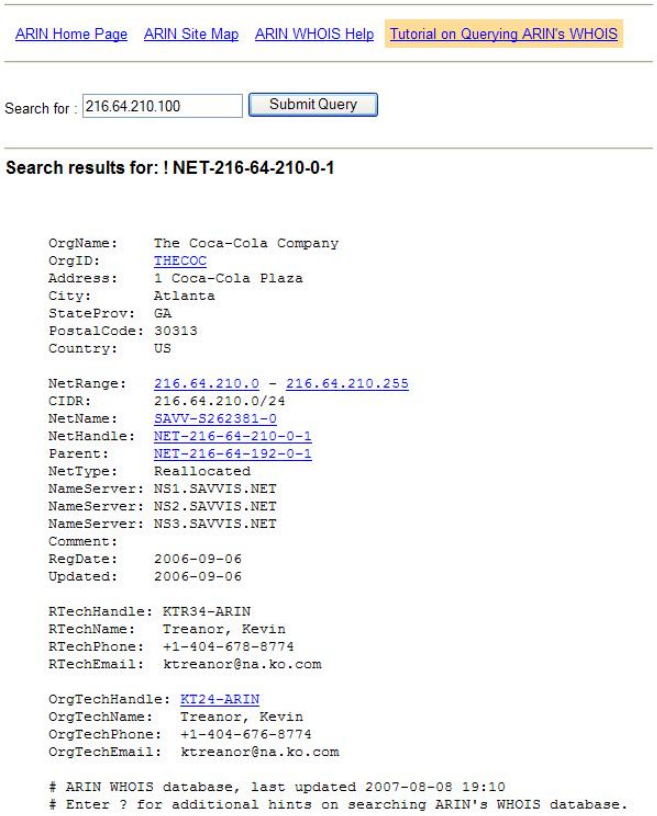
Geolocation: Core To The Local Space And Key To Click-Fraud Detection
by Chris Silver Smith
Search Engine Land
http://searchengineland.com/geolocation-core-to-the-local-space-and-key-to-click-fraud-detection-11922
Aug 13, 2007 at 8:20am ET

…How it works

At its most basic, online geolocation we're referring to is an attempt to identify the actual physical location of internet users. There are a few different ways that this may be accomplished. The best-known method is to take the user's IP address, which is transmitted with every internet request, and to look up the organization and physical address listed as the owner of that IP address. Anyone can do this, by querying the Whois information at ARIN – the American Registry for Internet Numbers. (Note: this is NOT the same as a domain name Whois query! Many IP addresses may not be associated with a domain name at all, so a domain name Whois of an IP address may not get you geolocation info.)

For instance, let's say that I noticed that a visitor to my website came in on IP address 216.64.210.100, according to my server's log files. I can query ARIN for that IP address, and I see that it's an address included within a block of IP addresses owned by The Coca-Cola Company:

Output from ARIN WHOIS



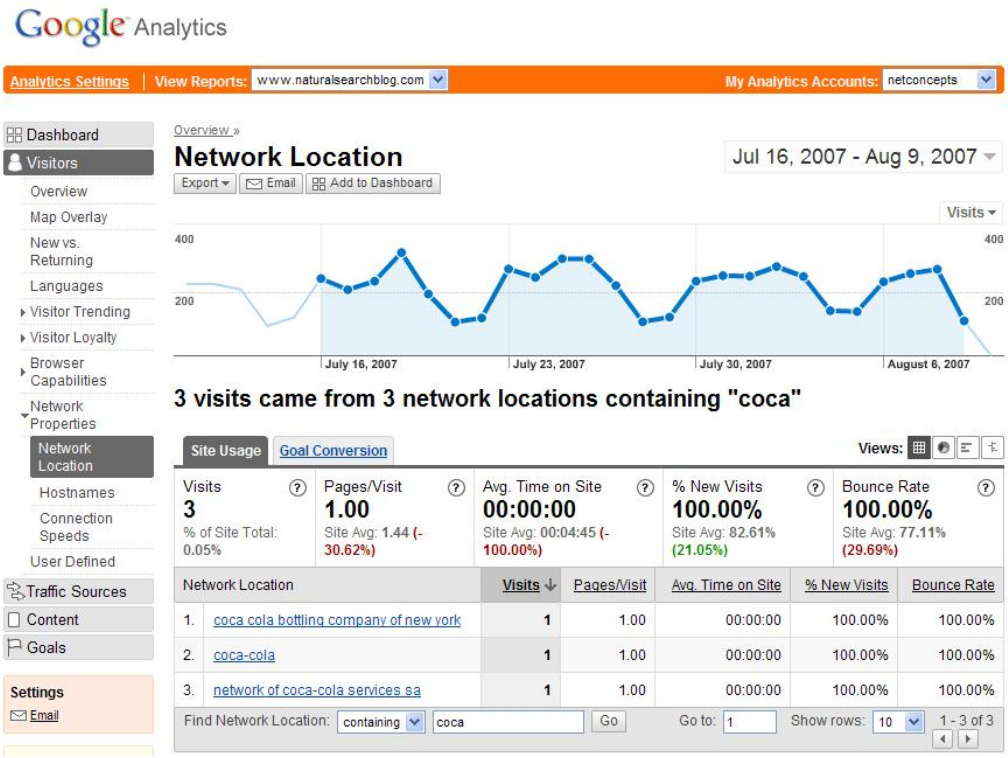
ARIN Home Page | ARIN Site Map | ARIN WHOIS Help | Tutorial on Querying ARIN's WHOIS

Search for : 216.64.210.100 [Submit Query]

Search results for: ! NET-216-64-210-0-1

```
OrgName:    The Coca-Cola Company
OrgID:      THECOC
Address:    1 Coca-Cola Plaza
City:       Atlanta
StateProv:  GA
PostalCode: 30313
Country:    US

NetRange:   216.64.210.0 - 216.64.210.255
CIDR:       216.64.210.0/24
NetName:    SAVV-S262381-0
NetHandle:  NET-216-64-210-0-1
Parent:     NET-216-64-192-0-1
NetType:    Reallocated
NameServer: NS1.SAVVIS.NET
NameServer: NS2.SAVVIS.NET
NameServer: NS3.SAVVIS.NET
Comment:
RegDate:    2006-09-06
Updated:    2006-09-06

RTechHandle: KTR34-ARIN
RTechName:   Treanor, Kevin
RTechPhone:  +1-404-678-8774
RTechEmail:  ktreanor@na.ko.com

OrgTechHandle: KT24-ARIN
OrgTechName:   Treanor, Kevin
OrgTechPhone:  +1-404-676-8774
OrgTechEmail:  ktreanor@na.ko.com

# ARIN WHOIS database, last updated 2007-08-08 19:10
# Enter ? for additional hints on searching ARIN's WHOIS database.
```

I could then perhaps figure that this visitor was an employee of The Coca-Cola Company, perhaps reading an article in the series of pieces I recently did about the Coca-Cola website. Indeed, my Google Analytics report is showing that I got a few visits from people associated with Coca-Cola during that time:



Since I can identify visitors from The Coca-Cola Company, I could deliver up content specific to them – I've heard stories about Google and Yahoo delivering up ads for engineering positions to the employees of Microsoft in Redmond using this method, for instance. More importantly, I can now assume that this user is likely to be physically located in Atlanta, Georgia—so I know their City, State, Zip Code, Designated Metro Area, and Country!

Naturally, it's likely not feasible to automatically perform an ARIN lookup with each visitor to your website before delivering up data, because it would take too long. So, there are a few companies out there who are aggregating and caching the network data and either providing lookup tables or web service lookups to those who wish to deliver location-specific content or who are using the data for reporting or fraud detection purposes.

Some ISPs which provide internet access through hotels may now be providing the physical locations of their networks of access points to the geolocation data aggregators as well, and in many cases these ISPs are hosting the default web page portals of local information to the hotel visitors. Some ISPs may also be quietly providing geolocational data to the aggregators as well, allowing all their customers to be geolocated to varying degrees.

Also, internet service providers who host Wi-Fi hotspots throughout the world are providing data to various of these aggregators, allowing the hotspots' IP addresses to be associated with precise physical addresses.

Mobile phones are able to be geolocated by triangulating their location from area cell phone towers, and there are increasing numbers of wireless devices such as phones, PDAs, and laptops which are getting integrated with GPS satellite pinpointing, paving the way to associate precise

coordinates with them. As more mobile devices like the iPhone leverage Wi-Fi access, there will be a variety of geolocational methods which will be able to pinpoint mobile users.

Who provides the geolocation data?

Quova is considered the best-in-class (probably with a price tag to match) of the geolocation data aggregators, and their data is apparently used by Google, Yahoo!, and MSN to geotarget content and ads, and likely for the purposes of analytics and fraud detection as well. They were founded in 2000 and they geolocate users through IP address location data as well as tracing network gateways and router locations. They also likely traceroute users coming through proxies to better determine location to some degree, and they analyze request latency of users passing through proxies to help determine physical distance from the proxy servers' physical locations.

Quova recently partnered with Mexens Technology in order to supplement their IP/network location data with Wi-FI hotspot locations, device GPS, and wireless tower triangulation.

Quova uses Pricewaterhouse Coopers to audit their geolocation data, and are perhaps the only company allowing independent, third-party validation testing of this sort. Their GeoDirectory Data Sheet states that PwC does this auditing by testing Quova data against "…large, independent third-party data sets of actual web users…". I interpret that to mean that PwC likely obtains IP addresses from some ISPs who tell them the countries and states associated with the IP addresses, and they check to see how accurately the Quova data identifies the locations of those addresses….

[the article discusses some other vendors of geolocation information]

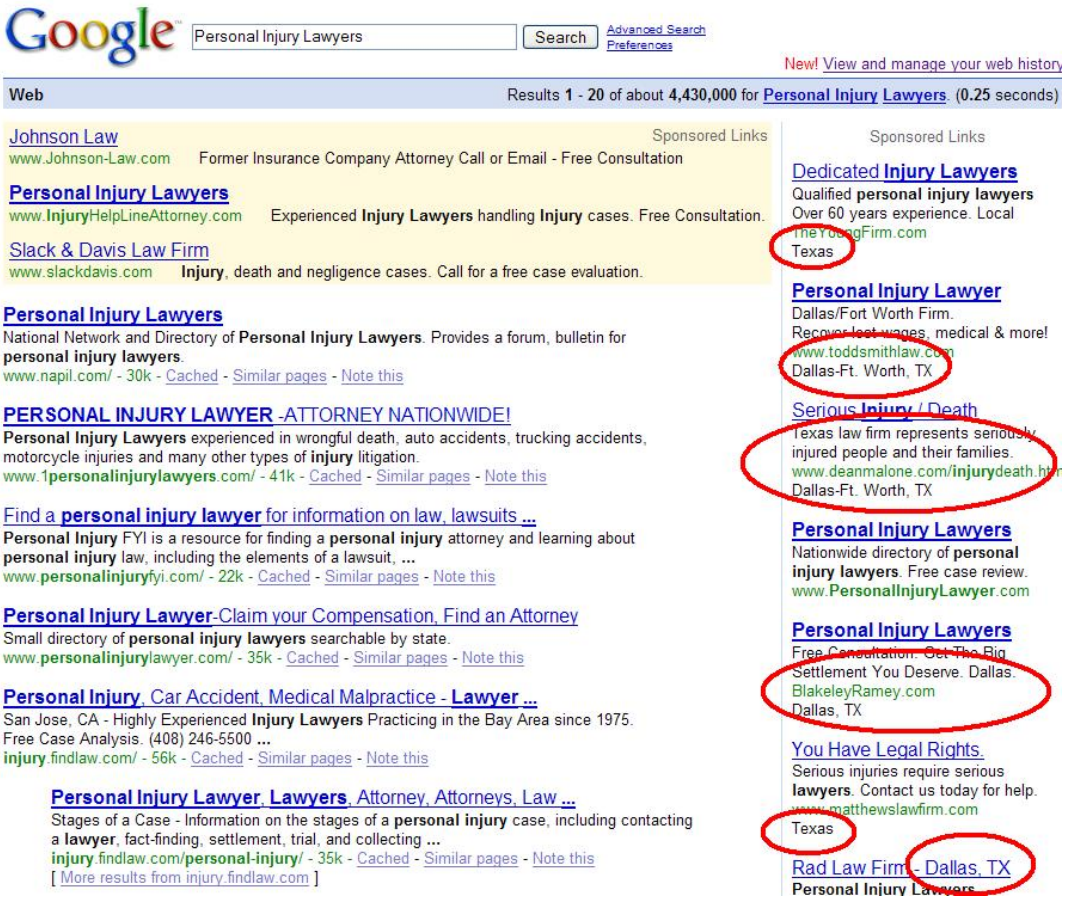
I've just touched on some of the companies that are most-interesting to me who are providing geolocation products and services. There are likely quite a number of companies which are also doing this in-house to some degree. For instance, I wouldn't be surprised if Google wasn't geolocating through querying and caching of ARIN data on top of data they're receiving from other providers listed above. Considering how vital geolocation data is to the policing of click-fraud, Google could be building out their own complete geolocation data aggregation infrastructure. Further, it's also been suggested that Google is likely using domain's registration data through Google's status as a registrar to assist in associating websites with geographic locations for Google Maps—not precisely the geolocation of users I'm covering here, but a closely related method that could be useful to local SEO.

Many mobile service providers are also using the geolocational information associated with their devices in order to deliver up location-specific information on their own, without the assistance of the geolocation data aggregators.

How geolocation is used in the local space and in general internet marketing:

Targeting Ads to user's locality – ads could be targeted by varying levels of locality including ZIP Code, City, Metro Area (DMA), Region, State, Company, Country, and Time Zone. For example, I just performed a search in Google for "personal injury lawyers", and you can see that

they displayed a number of ads for lawyers who've targeted ads to the Dallas, Texas metro area where I'm writing this article:



Targeting locally apropos content to users, including language delivery, currency such as pounds/euros/dollars/yen/etc—providing native users' currency on e-com pages and order forms, location-specific text/images, customization of web search results which may have a local component, automating Store Locator pages for retailers, etc.

Content Restriction: there are frequently some contractual/legal limits on what products and services can be sold where. Uses include restricting online gambling from US users; enforcement of trade embargoes so that certain items won't be sold to countries disallowed by federal laws; some items can only be sold in particular areas of the world and some promotional contests are only allowed by certain states or provincial rules.

Financial Fraud Detection: denying sales to possibly compromised credit cards or bank accounts – for instance, if the IP address of the online user is in suspect foreign country, but account owner address is in the US.

Identity Fraud Detection: geolocation provides additional signal for logins for protecting user identities.

Advertising Fraud Detection: filtering out invalid or fraudulent clicks – products/services only available in one country, but Pay-Per-Click advertising clicks are coming from another.

Potential Detection of DoS Attacks: many requests coming in from a wide variety of natural-looking IP addresses, but geolocation of requestors shows requests actually coming all from one primary location.

Internet Analytics Applications: analyzing and showing from where visitors viewed a website, and quantifying how many come from particular locations.

Site Server Locations for SEO: there's some supposition that websites hosted in the country who's audience they're targeting might actually get better rankings within search engines targeting that country's users.

The issue of error rates

From the very beginning, geolocation providers have been asked about how much error is involved in their ability to pinpoint web users, and from the very beginning geodata consumers have noticed some amount of errors happening. There are a lot of anecdotal tales of ads and content being incorrectly displayed for users when their geolocation has been incorrectly assessed.

The classic example of IP locating error is caused where a large internet service provider may provide web access across the world, but the block of their users' IP addresses are all associated with the ISP's corporate headquarters or network office in one location. With simplistic IP address mapping, all those users could be geolocated by aggregators to that single corporate office location, even though they might in actuality be spread out in many areas. The most famous example of this is the AOL proxy server issue wherein geolocation aggregators were originally unable to pinpoint AOL users and incorrectly associating them all with their Virginia address.

Quova used to claim to have beat the AOL proxy barrier to identify where their requests originate, but specific terminology touting this ability has been considerably toned down these days in Quova's collateral materials, and their GeoDirectory data sheet merely mentions that they have included a flag for AOL. One assumes that their confidence factors rating for geolocation and general proxy detection/locating ability might be used to give some level of AOL user identification ability, but the flag must be provided so that the geodata consumers could opt to not geolocate AOL users if they presumed the data to be too error-prone.

While the AOL proxy issue is the most famous, many other ISPs likely have some similar barriers to pinpointing their users. Using one of the previously-mentioned geolocation services, I just now checked my IP address and was mapped to Keller, Texas, even though I'm writing this 20 miles away. Large corporations likely have this going on as well. For instance, in the Coca-Cola IP address example I gave above, I'd bet that the company is large enough that they probably have offices throughout the states and world, and their employees addresses might be prone to being incorrectly mapped to their headquarters locations.

Since IP address mapping using ARIN registrar data could be so prone to error at the more granular levels, a number of the geolocation providers rush to quote accuracy estimates based on the broader, country and regional levels:

> Quova: "…In audited tests using large, independent third-party data sets of actual web users, Quova's country level accuracy was measured at 99.9%. US state level accuracy was measured at approximately 95%."
>
> IP2Location: "…over 95 percent matching accuracy at the country level…"

Another factor occurs when users specifically choose to route their requests through a proxy in order to anonymize their internet usage, either for privacy reasons, or for the sake of hiding criminal activities. A number of sites out there provide free or paid anonymizing services, allowing users to submit their internet requests which then get filtered through another layer of services before the requests reach content providers' servers.

Obviously, geolocation accuracy could be more accurate through network route mapping and enhancing IP registration data with data from the large ISPs, along with Wi-Fi and mobile device location data.

Users browsing the internet through mobile phones and other wireless devices now pose an additional proxying problem, since most of the wireless carriers will display only a central IP address for all of their users, and any attempts at network routing will be stymied by the fact that wireless network traffic isn't being monitored. For the companies who are providing content through these wireless carriers' mobile portals, they may be supplied geolocation info by the carriers, but this may not help most webmasters who don't have such partnerships. As more mobile device users demand open access to the entire internet, the mobile carrier's proxies may become an increasing source of error in geolocation data.

Freshness of data weighs in as well since IP address blocks change over time, so if an IP location source doesn't update their database, it can result in incorrect targeting, just as with this incident related by Barry Schwartz where a Texas school district kept getting content from Google Canada.

The biggest problem in assessing the error rates of geolocation data is the simple fact that there's no way to really test well for accuracy. The one and only company which publicly states that it uses external auditing (Quova), provided by Pricewaterhouse Coopers, is apparently testing by comparing their geodata with large datasets where they know the physical locations of the users associated with the IP addresses. But, how broad is that comparison data? Is the testing comparison working the same as when users are dynamically being geotargeted through the data in real-time? Does data from just a few major ISPs (assuming that's what's being used) really represent the majority of internet users? Does it take into account the huge amount of corporate employees browsing during their workdays? (I'd guess not, since most large corporations probably shouldn't be sharing the locational information associated with their employee's IP addresses.) What's the estimate for accuracy at the city-level and postal-code level?

At best, this is only an estimation and not direct test results for accuracy, so we don't know what the error rate really is.

To be fair, it's simply not possible for any of us to know the actual error rates involved, since it's impossible to assess whether all internet users are being accurately geolocated through any of these services. We can only sample some amount of users, and decide whether that sample set should be considered representative of all usage or not.

On one hand, this inability to assess error rates more precisely is highly concerning, particularly for the paid search industry, since it makes the entire policing structure of click fraud appear to be built upon a house of cards.

On the other hand, the filtering of suspect clicks is primarily based upon identifying the country where the click is originating. Countries with higher apparent rates of fraudulent clicks tend to be flagged as less-trustable, and those clicks are discounted from billing. Based on the logic that most ISPs are fairly country-specific, and that most large companies might use completely different IP address blocks for their employees in different countries, I'm willing to believe the industry's published accuracy rates of 99.9% to 95% at country-level geolocation. But, when you're speaking in terms of processing billions upon billions of clicks, and millions of dollars, 5% to 0.1% can still amount to a whole lot of money…

Even considering the higher accuracy of country/regional geolocation, there's still cause for concern for advertisers who are buying ads and targeting at the more granular levels—are their ads being shown to the right demographic groups, and are their clicks coming from the qualified buyers they're seeking? The more granular levels of geolocation are apparently still considered to be much more error-prone, and the industry remains quiet about it.

Other downsides to use of geolocation:

Geolocation is probably a very bad method for targeting languages! Better to use content negotiation through browsers, using the language-accept headers to choose which languages to display to users (this is what the W3C recommends). While using geolocation to choose which language to deliver up to an user, search engine spiders may all come in from a central location or from one of their regional data centers, so using geolocation for language targeting would not be best practice and could result in less-optimal natural search marketing.

Even delivering up local-oriented content by geolocation of users can be dicey, if one doesn't properly handle search engine spiders. Last year, I informed representatives from Amazon.com on how their geolocation for the purpose of delivering up their yellow pages links was ruinous to their SEO of that section, since Googlebot was apparently being delivered up all Washington, D.C. content, keeping the rest of their national content unavailable for indexing. Geolocation can be great for targeting content to users, but design a default for unidentifiable users and search engine bots.

Geolocation can creep out users who don't understand how it works and can raise user privacy concerns. Most users still don't realize their physical locations are being mapped while they're browsing, so many still don't quite know enough about the technology to be concerned. The industry hasn't really addressed this as well as it could. Quova's FAQ is rather dismissive of privacy concerns, saying only "Since accuracy is limited to zip code level, Quova does not pinpoint individual user locations…", though this seems a bit inaccurate since they are also apparently incorporating GPS, Wi-Fi, and wireless tower triangulation through Mexens Technology – meaning the pinpointing of users could be a whole lot more accurate than mere ZIP code level.

Geolocation can reveal some information you wanted to keep confidential, which is why it should be on the radar screens of privacy advocates. Don't want your competitors knowing you're examining some of their pages every day? If you're viewing from a unique city where average users are unlikely to be viewing your competitor's site pages, you might want to try dialing up through an ISP outside of your town or going through a distant proxy or two before viewing their pages, just to try to obscure your geolocation info. Or, call up a friend in another state to send you screen-grabs of the site.

For travel-based industries, filtering out PPC clicks from suspect foreign countries could result in undercounting of valid consumer traffic. That's cool if you're a travel business advertising in PPC networks, since it may get you more free ads and higher apparent conversion rates. But, it's not so cool for the ad network companies and publishers displaying those ads – they're likely getting a little less revenue than they should since some of the "good" traffic is inevitably going to be thrown away with the "bad".

Summary

Geolocation is here to stay in the online local space. Its use in fraud detection and regulatory compliance is only deepening, and geolocation reporting in web analytics has become a standard. Geolocation data is a necessity for the geotargeting of ads, and that would appear to be an increasingly popular choice amongst marketers as online advertising continues to gain traction among local businesses.

Geolocation use in targeting relevant content to users is still in something of an experimental stage, and few sites seem to be really making simultaneously extensive and effective use of it.

It should not really be used in content mediation for delivering different languages, since this likely will not allow the various translations of the site pages to be properly indexed in the search engines for various countries/tongues.

Geolocation may have a factor in effective SEO—anecdotal evidence and logical reasoning would indicate that it could make sense that a site hosted within a particular country might be more relevant to that country's citizens than in other countries. I would guess that this factor wouldn't apply as much for higher-PR sites or publicly-traded companies, but there's not a lot of research evidence out there.

The biggest issue with geolocation is the lack of transparency in how the aggregators are gathering the data, and how high the error rates may be with all the levels of granularity. The geolocation providers all desire to keep their methods proprietary, but this competitive need for confidentiality makes it difficult for companies to try to estimate relative levels of accuracy amongst the providers. Many companies may be using cheaper providers than they should for the purposes of advertising click-fraud detection, leaving themselves open to liability of fraud claims, and causing innocent advertisers to be paying higher amounts than they should. Considering how geolocation has become such a major component of the policing of click-fraud, it's surprising that there hasn't been a wider demand for transparency and standardized methods for testing accuracy. The leaders in the industry should pursue a greater degree of openness and a greater variety of auditing methods to check accuracy.

Toys 'R' Us, Inc. v . Step Two, S.A., 318 F.3d 446 (3d Cir. 2003)
Oberdorfer, District Judge.

Toys 'R' Us, Inc. and Geoffrey, Inc. ("Toys") brought this action against Step Two, S.A. and Imaginarium Net, S.L. ("Step Two"), alleging that Step Two used its Internet web sites to engage in trademark infringement, unfair competition, misuse of the trademark notice symbol, and unlawful "cybersquatting," in violation of the Lanham Act, 15 U.S.C. § 1501 et seq., and New Jersey state law. The District Court denied Toys' request for jurisdictional discovery and, simultaneously, granted Step Two's motion to dismiss for lack of personal jurisdiction. We hold that the District Court should not have denied Toys' request for jurisdictional discovery. We therefore reverse and remand for limited jurisdictional discovery, relating to Step Two's business activities in the United States, and for reconsideration of personal jurisdiction with the benefit of the product of that discovery, with a view to its renewing administration of the case, in the event the District Court finds that it does have jurisdiction.

I.

Toys, a Delaware corporation with its headquarters in New Jersey, owns retail stores worldwide where it sells toys, games, and numerous other products. In August 1999, Toys acquired Imaginarium Toy Centers, Inc., which owned and operated a network of "Imaginarium" stores for the sale of educational toys and games. As part of this acquisition, Toys acquired several Imaginarium trademarks, and subsequently filed applications for the registration of additional Imaginarium marks. Prior to Toys' acquisition, the owners of the Imaginarium mark had been marketing a line of educational toys and games since 1985 and had first registered the Imaginarium mark with the United States Patent and Trademark Office in 1989. Toys currently owns thirty-seven freestanding Imaginarium stores in the U.S., of which seven are located in New Jersey. In addition, there are Imaginarium shops within 175 of the Toys "R" Us stores in the U.S., including five New Jersey stores.

Step Two is a Spanish corporation that owns or has franchised toy stores operating under the name "Imaginarium" in Spain and nine other countries. It first registered the Imaginarium mark in Spain in 1991, and opened its first Imaginarium store in the Spanish city of Zaragoza in November 1992. Step Two began expanding its chain of Imaginarium stores by means of a franchise system in 1994. It has registered the Imaginarium mark in several other countries where its stores are located. There are now 165 Step Two Imaginarium stores. The stores have the same unique facade and logo as those owned by Toys, and sell the same types of merchandise as Toys sells in its Imaginarium stores. However, Step Two does not operate any stores, maintain any offices or bank accounts, or have any employees anywhere in the United States. Nor does it pay taxes to the U.S. or to any U.S. state. Step Two maintains that it has not directed any advertising or marketing efforts towards the United States. The record does, however, indicate some contacts between Step Two and the United States: for example, a portion of the merchandise sold at Step Two's Imaginarium stores is purchased from vendors in the United States. Additionally, Felix Tena, President of Step Two, attends the New York Toy Fair once each year.

In the mid-1990s, both parties turned to the Internet to boost their sales. In 1995, Imaginarium Toy Centers, Inc. (which Toys later acquired) registered the domain name <imaginarium.com> and launched a web site featuring merchandise sold at Imaginarium stores. In 1996, Step Two registered the domain name <imaginarium.es>, and began advertising merchandise that was available at its Imaginarium stores. In April 1999, Imaginarium Toy Centers registered the domain name <imaginarium.net>, and launched another web site where it offered Imaginarium merchandise for sale. In June 1999, Step Two registered two additional "Imaginarium" domain names, <imaginariumworld.com> and <imaginarium-world.com>. In May 2000, Step Two registered three more domain names: <imaginariumnet.com>, <imaginariumnet.net>, and <imaginariumnet.org>. Step Two's web sites are maintained by Imaginarium Net, S.L., a subsidiary of Step Two, S.A. formed in 2000.

At the time this lawsuit was filed, four of the aforementioned sites operated by Step Two were interactive, allowing users to purchase merchandise online. When buying merchandise via Step Two's web sites, purchasers are asked to input their name and email address, as well as a credit card number, delivery address, and phone number. At no point during the online purchase process are users asked to input their billing or mailing address. The web sites provide a contact phone number within Spain that lacks the country code that a user overseas would need to dial. Moreover, the prices are in Spanish pesetas and Buros, and goods ordered from those sites can be shipped only within Spain. Step Two's Imaginarium web sites are entirely in Spanish.

Visitors to the four sales-oriented Step Two web sites may elect to receive an electronic newsletter, or sign up for membership in "Club Imaginarium," a promotional club with games and information for children. Each registrant for Club Imaginarium is required to provide a name and an email address. At the time this suit was filed, there was a section for "voluntary information," including the registrant's home address, on the Club Imaginarium registration page. This optional portion of the page required users to choose from a pull-down list of Spanish provinces, and did not accommodate mailing addresses in the United States. After joining Club Imaginarium via the web site, registrants receive an automatic email response.

Mr. Tena submitted an affidavit stating that Step Two had not made any sales via its web sites to U.S. residents. Toys, however, adduced evidence of two sales to residents of New Jersey conducted via Step Two's Imaginarium web sites. These purchases were initiated by Toys. Lydia Leon, a legal assistant in the Legal Department of Geoffrey, Inc., made the first purchase. Ms. Leon, a resident of New Jersey, purchased a toy via <www.imaginariumworld.com> on January 23, 2001. The second purchase was made in February 2001 by Luis M. Lopez, an employee of Darby & Darby P.C., attorneys for Toys. Mr. Lopez is also a resident of New Jersey, and accessed <www.imaginarium.es> to make his purchase.

For both of these sales, the items were shipped to Angeles Benavides Davila, a Toys employee in Madrid, Spain; Ms. Benavides Davila then forwarded the items to the offices of Geoffrey, Inc. in New Jersey. Both purchases were made with credit cards issued by U.S. banks. Additionally, both purchasers received in New Jersey an email confirming their purchases, and a subsequent email with a login and password to access Club Imaginarium. One of the two purchasers also separately registered for Club Imaginarium, exchanged emails with a Step Two employee about his purchase, and received a copy of an email newsletter from Step Two. Aside from these two

sales, there is no evidence in the record of a sale to anyone in the United States. After learning of these two sales, Mr. Tena submitted a second affidavit stating that his company does not know where its purchasers reside, as that information is not apparent from a purchaser's email address, and Step Two keeps records only of shipping addresses….

II.

In the following discussion, we first consider the standard for personal jurisdiction based upon a defendant's operation of a commercially interactive web site, as articulated by courts within this circuit and other Courts of Appeals. In light of that standard and the arguments presented in the proceeding below, we then assess the propriety of the District Court's denial of jurisdictional discovery.

A. Personal Jurisdiction Based on the Operation of a Web Site

The advent of the Internet has required courts to fashion guidelines for when personal jurisdiction can be based on a defendant's operation of a web site. Courts have sought to articulate a standard that both embodies traditional rules and accounts for new factual scenarios created by the Internet. Under traditional jurisdictional analysis, the exercise of specific personal jurisdiction requires that the "plaintiff's cause of action is related to or arises out of the defendant's contacts with the forum." Beyond this basic nexus, for a finding of specific personal jurisdiction, the Due Process Clause of the Fifth Amendment requires (1) that the "defendant ha[ve] constitutionally sufficient 'minimum contacts' with the forum," id. (quoting Burger King Corp. v. Rudzewicz, 471 U.S. 462, 474 (1985)), and (2) that "subjecting the defendant to the court's jurisdiction comports with 'traditional notions of fair play and substantial justice,'" id. (quoting Int'l Shoe Co. v. Washington, 326 U.S. 310, 316 (1945)). The first requirement, "minimum contacts," has been defined as "'some act by which the defendant purposefully avails itself of the privilege of conducting activities within the forum State, thus invoking the benefits and protections of its laws.'" Asahi Metal Indus. Co., Ltd. v. Superior Court of California, 480 U.S. 102, 109 (1987) (quoting Burger King Corp., 471 U.S. at 475). Second, jurisdiction exists only if its exercise "comports with traditional notions of fair play and substantial justice," i.e., the defendant "should reasonably anticipate being haled into court" in that forum. World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 297 (1980).

The precise question raised by this case is whether the operation of a commercially interactive web site accessible in the forum state is sufficient to support specific personal jurisdiction, or whether there must be additional evidence that the defendant has "purposefully availed" itself of the privilege of engaging in activity in that state. Prior decisions indicate that such evidence is necessary, and that it should reflect intentional interaction with the forum state. If a defendant web site operator intentionally targets the site to the forum state, and/or knowingly conducts business with forum state residents via the site, then the "purposeful availment" requirement is satisfied. Below, we first review cases from this and other circuits that articulate this requirement. Next, we consider the role of related non-Internet contacts in demonstrating purposeful availment. We then assess whether the "purposeful availment" requirement has been satisfied in the present case.

1. The “Purposeful Availment” Requirement in Internet Cases

a. Third Circuit Cases

The opinion in Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997) has become a seminal authority regarding personal jurisdiction based upon the operation of an Internet web site. The court in *Zippo* stressed that the propriety of exercising jurisdiction depends on where on a sliding scale of commercial interactivity the web site falls. In cases where the defendant is clearly doing business through its web site in the forum state, and where the claim relates to or arises out of use of the web site, the Zippo court held that personal jurisdiction exists. In reaching this conclusion, the Zippo court relied on CompuServe, Inc. v. Patterson, 89 F.3d 1257 (6th Cir. 1996), which found the exercise of personal jurisdiction to be proper where the commercial web site’s interactivity reflected specifically intended interaction with residents of the forum state.

Analyzing the case before it, the *Zippo* court similarly underscored the intentional nature of the defendant’s conduct vis-a-vis the forum state. In *Zippo*, the defendant had purposefully availed itself of doing business in Pennsylvania when it “repeatedly and consciously chose to process Pennsylvania residents’ applications and to assign them passwords,” knowing that the contacts would result in business relationships with Pennsylvania customers. The court summarized the pivotal importance of intentionality as follows:

> When a defendant makes a conscious choice to conduct business with the residents of a forum state, ‘it has clear notice that it is subject to suit there.’ ... If [the defendant] had not wanted to be amenable to jurisdiction in Pennsylvania, ... it could have chosen not to sell its services to Pennsylvania residents.

Since *Zippo*, several district court decisions from this Circuit have made explicit the requirement that the defendant intentionally interact with the forum state via the web site in order to show purposeful availment and, in turn, justify the exercise of specific personal jurisdiction. As another district court in this Circuit put it, “[c]ourts have repeatedly recognized that there must be ‘something more’ ... to demonstrate that the defendant directed its activity towards the forum state.”

b. Case Law from Other Circuits

Several Courts of Appeals decisions have adopted “purposeful availment” requirements that are consistent with the principles articulated in the Zippo line of cases. The Fourth Circuit, in ALS Scan v. Digital Service Consultants, Inc., 293 F.3d 707 (4th Cir. 2002), expressly incorporated an “intentionality” requirement when fashioning a test for personal jurisdiction in the context of the Internet:

> a State may, consistent with due process, exercise judicial power over a person outside of the State when that person (1) directs electronic activity into the State, (2) with the manifested intent of engaging in business or other interactions within

> the State, and (3) that activity creates, in a person within the State, a potential cause of action cognizable in the State's courts.

In Cybersell, Inc. v. Cybersell, Inc., 130 F.3d 414 (9th Cir. 1997), the Ninth Circuit considered an infringement action brought against a Florida web site operator whose allegedly infringing site was accessible in Arizona, the state where the plaintiff had its principal place of business. In declining to exercise specific personal jurisdiction, the *Cybersell* court found there must be "'something more' [beyond the mere posting of a passive web site] to indicate that the defendant purposefully (albeit electronically) directed his activity in a substantial way to the forum state." Decisions from other circuits have articulated similar standards. See, e.g., Neogen Corp. v. Neo Gen Screening, Inc., 282 F.3d 883, 890 (6th Cir. 2002) (holding that the purposeful availment requirement is satisfied "if the web site is interactive to a degree that reveals *specifically intended interaction* with residents of the state") (citation omitted) (emphasis added).

2. Non-Internet Contacts

In deciding whether to exercise jurisdiction over a cause of action arising from a defendant's operation of a web site, a court may consider the defendant's related non-Internet activities as part of the "purposeful availment" calculus. One case that relies on non-Internet contacts for the exercise of jurisdiction—a case Toys repeatedly cites—is Euromarket Designs, Inc. v. Crate and Barrel Ltd., 96 F. Supp. 2d 824 (N.D. Ill. 2000). In *Euromarket*, the court exercised jurisdiction over an Irish manufacturer based on its commercially interactive web site, even though the products purchased through the web site could not be shipped to Illinois. The court identified a number of non-Internet contacts between the defendant and Illinois, including the fact that the defendant's vendors included Illinois suppliers, its attendance at trade shows in Illinois, and its advertisement in publications that circulate in the United States (albeit originating outside). The *Euromarket* court also relied on the fact that the defendant billed Illinois customers, collected revenues from Illinois customers, and recorded sales from goods ordered from Illinois, and that the web site was designed to accommodate addresses in the United States.

Thus far, Toys has not shown that Step Two maintained the type of contacts that supported jurisdiction in *Euromarket*—i.e., that the defendant intentionally and knowingly transacted business with residents of the forum state, and had significant other contacts with the forum besides those generated by its web site. This limited record does not provide an occasion for us to spell out the exact mix of Internet and non-Internet contacts required to support an exercise of personal jurisdiction. That determination should be made on a case-by-case basis by assessing the "nature and quality" of the contacts. However, non-internet contacts such as serial business trips to the forum state, telephone and fax communications directed to the forum state, purchase contracts with forum state residents, contracts that apply the law of the forum state, and advertisements in local newspapers, may form part of the "something more" needed to establish personal jurisdiction. It is noteworthy that the Supreme Court in *Burger King Corp*., when expounding on the "minimum contacts" requirement, referred generally to a defendant's "activities" in the forum state—a term that includes the aforementioned non-Internet contacts.

3. Personal Jurisdiction over Step Two

As *Zippo* and the Courts of Appeals decisions indicate, the mere operation of a commercially interactive web site should not subject the operator to jurisdiction anywhere in the world. Rather, there must be evidence that the defendant "purposefully availed" itself of conducting activity in the forum state, by directly targeting its web site to the state, knowingly interacting with residents of the forum state via its web site, or through sufficient other related contacts.

Based on the facts established in this case thus far, Toys has failed to satisfy the purposeful availment requirement. Step Two's web sites, while commercial and interactive, do not appear to have been designed or intended to reach customers in New Jersey. Step Two's web sites are entirely in Spanish; prices for its merchandise are in pesetas or Euros, and merchandise can be shipped only to addresses within Spain. Most important, none of the portions of Step Two's web sites are designed to accommodate addresses within the United States. While it is possible to join Club Imaginarium and receive newsletters with only an email address, Step Two asks registrants to indicate their residence using fields that are not designed for addresses in the United States.

Moreover, the record may not now support a finding that Step Two knowingly conducted business with residents of New Jersey. The only documented sales to persons in the United States are the two contacts orchestrated by Toys, and it appears that Step Two scarcely recognized that sales with U.S. residents had been consummated.[5]

At best, Toys has presented only inconclusive circumstantial evidence to suggest that Step Two targeted its web site to New Jersey residents, or that it purposefully availed itself of any effort to conduct activity in New Jersey. Many of the grounds for jurisdiction that Toys advanced below have been deemed insufficient by the courts. First, the two documented sales appear to be the kind of "fortuitous," "random," and "attenuated" contacts that the Supreme Court has held insufficient to warrant the exercise of jurisdiction. As for the electronic newsletters and other email correspondence, "telephone communication or mail sent by a defendant [do] not trigger personal jurisdiction if they 'do not show purposeful availment.'" The court in *Barrett* found that the exchange of three emails between the plaintiff and defendant regarding the contents of the defendant's web site, without more, did not "amount to the level of purposeful targeting required under the minimum contacts analysis." Non-Internet contacts, such as Mr. Tena's visits to New York and the relationships with U.S. vendors, have not been explored sufficiently to determine whether they are related to Toys' cause of action, or whether they reflect "purposeful availment."

[5] Toys argues that Step Two was aware that it was conducting business with New Jersey residents. In particular, Toys points to the email correspondence between Mr. Luis M. Lopez and a representative of Step Two regarding Mr. Lopez's overpayment. Mr. Lopez requested that the difference be mailed to his home address in "South Orange, NJ 07079," but did not spell out "New Jersey" or specify that he resided in the United States. The Step Two representative, apparently uncertain about the address, sent a reply stating "I have received your address and as far as I can see, it is pretty far from here (we are in Zaragoza). I would appreciate your giving me more information on the address so that I can be sure that it will arrive." Mr. Lopez's response to this message—if he sent one—is not included in the record. Although Step Two ultimately learned that Mr. Lopez is a United States resident, a trier of fact could reasonably find from the correspondence that the company did not contemplate that sales would occur with U.S.-based purchasers.

Absent further evidence showing purposeful availment, Toys cannot establish specific jurisdiction over Step Two.[6] However, any information regarding Step Two's intent vis-a-vis its Internet business and regarding other related contacts is known by Step Two, and can be learned by Toys only through discovery. The District Court's denial of jurisdictional discovery is thus a critical issue, insofar as it may have prevented Toys from obtaining the information needed to establish personal jurisdiction. We next turn to whether the District Court properly denied Toys' request for jurisdictional discovery.

B. Jurisdictional Discovery…

Toys requested jurisdictional discovery for the purpose of establishing either specific personal jurisdiction, or jurisdiction under the federal long-arm statute, Fed. R. Civ. P. 4(k)(2).[7] The District Court denied Toys' request, explaining that "the clear focus of the Court is directed, as it should be, to the web site[,] [a]nd to the activity of the defendants related to that web site, which is making sales here, ..." The court added that "the apparent contradictions, if such there will be in the Tena affidavit, [and] what else Mr. Tena might have been doing here, just have no relationship to where the eye is directed and should stay and that is, the web site activities of this defendant."

We are persuaded that the District Court erred when it denied Toys' request for jurisdictional discovery. The court's unwavering focus on the web site precluded consideration of other Internet and non-Internet contacts-indicated in various parts of the record-which, if explored, might provide the "something more" needed to bring Step Two within our jurisdiction. Although the plaintiff bears the burden of demonstrating facts that support personal jurisdiction, courts are to assist the plaintiff by allowing jurisdictional discovery unless the plaintiff's claim is "clearly frivolous." If a plaintiff presents factual allegations that suggest "with reasonable particularity" the possible existence of the requisite "contacts between [the party] and the forum state," the plaintiff's right to conduct jurisdictional discovery should be sustained.

Where the plaintiff has made this required threshold showing, courts within this Circuit have sustained the right to conduct discovery before the district court dismisses for lack of personal jurisdiction. Here, instead of adopting a deferential approach to Toys' request for discovery, the District Court appears to have focused entirely on the web site, thereby preventing further inquiry into non-Internet contacts.

---

[6] As an alternative to the "minimum contacts" analysis for specific jurisdiction, Toys argues that jurisdiction over Step Two may be based on the "effects" test. Following the lead of the Supreme Court in Calder v. Jones, 465 U.S. 783, 788-89 (1984), the Third Circuit has held that personal jurisdiction may, under certain circumstances, be based on the effects in the forum state of a defendant's tortious actions elsewhere. One of the Third Circuit's requirements is that the "defendant expressly aimed his tortious conduct at the forum...."

Even assuming that Step Two's registration of the Imaginarium domain names and its operation of web sites under that name bring about an injury to Toys in New Jersey (its corporate headquarters), Toys has failed to establish that Step Two engaged in intentionally tortious conduct expressly aimed at New Jersey. In the present case, this intentionality requirement is the key missing component for jurisdiction under either the "minimum contacts" analysis or the "effects" test.

[7] The federal long-arm statute sanctions personal jurisdiction over foreign defendants for claims arising under federal law when the defendant has sufficient contacts with the nation as a whole to justify the imposition of U.S. law, but without sufficient contacts to satisfy the due process concerns of the long-arm statute of any particular state.

The record before the District Court contained sufficient non-frivolous allegations (and admissions) to support the request for jurisdictional discovery. First, Toys' complaint alleges that Step Two has "completely copied the IMAGINARIUM concept" from Toys. For example, Toys alleges that "the mix of toys sold by Step Two is identical to the mix of toys sold by Toys under the IMAGINARIUM mark," and that "Step Two continues to copy Toys' marketing developments and Intellectual property." Underlying Toys' complaint is its concern that Step Two is "attempt[ing] to expand [its] business throughout the world including the United States by operating international web sites that offer goods similar to the goods offered in Toy's [sic] IMAGINARIUM stores." Step Two's intent, according to Toys, is to "capitalize for [its] own pecuniary gain on the goodwill and excellent reputation of Toys...."

It is well established that in deciding a motion to dismiss for lack of jurisdiction, a court is required to accept the plaintiff's allegations as true, and is to construe disputed facts in favor of the plaintiff. Given the allegations as to Step Two's mimicry of Toys' ventures on the Internet and its copy-cat marketing efforts, it would be reasonable to allow more detailed discovery into Step Two's business plans for purchases, sales, and marketing. Limited discovery relating to these matters would shed light on the extent, if any, Step Two's business activity-including, but not limited to, its web site-were aimed towards the United States. This information, known only to Step Two, would speak to an essential element of the personal jurisdiction calculus.

Other aspects of the record should have also alerted the District Court to the possible existence of the "something else" needed to exercise personal jurisdiction. For example, Step Two concedes that a portion of the merchandise sold through its Imaginarium stores and web sites are purchased from U.S. vendors, and that Mr. Tena attends the New York Toy Fair each year. Further discovery into the vendor relationships and Mr. Tena's activities here, if any, may shed light on Step Two's intentions with respect to the U.S. market, or the extent of its business contacts in the United States. Discovery might also reveal whether these non-Internet contacts directly facilitate Step Two's alleged exploitation of Toys' marketing techniques by providing it with a supply of items identical to Toys' inventory to sell on its web sites.

The two documented sales to residents of New Jersey—and the subsequent emails sent from Step Two to the two purchasers—also speak "with reasonable particularity" to the possible existence of contacts needed to support jurisdiction. Although affiliates of Toys orchestrated the two sales, Mr. Tena's conflicting affidavits raise the possibility that additional sales to U.S. residents may have been conducted via the web sites. The need for additional discovery regarding sales is further underscored by the parties' uncertainty as to whether the residence of purchasers can be determined from their credit card number or through some other electronic means.[8]

Counsel for Toys mentioned some of these contacts when it explained to the District Court why it should be allowed jurisdictional discovery:

[8] In its brief on appeal, Step Two contends that Toys should not be allowed discovery because there is simply no basis for believing that there are any other contacts to find and, moreover, seeking discovery about other web site-generated contacts would be futile as Step Two does not keep track of billing addresses or the physical location of its email correspondents. At oral argument, however, counsel for Toys suggested there are means by which an individual's residence can be determined from a credit card number. Toys also suggests, in its brief on appeal, that the residence of on-line purchasers may be determined from the phone number that purchasers are required to input. These possibilities can be explored through discovery.

> Mr. Tena states in his affidavit that he has substantial regular and systematic contacts with the United States, [and] he attends trade shows. He purchases from vendors in the United States. I think at the very least, Your Honor, we should be able to inquire into what these substantial and continuing contacts are. Because apparently he buys a lot of the toys that he resells from U.S. vendors, because the ones that we have got were in English that we would be permitted to take discovery on that aspect. To determine whether or not ... he has made more sales within the State of New Jersey and in the United States as a whole, as far as accepting orders from United States residents. And/or whether there's a basis for general jurisdiction under Rule 4(k)(2), because of his regular and systematic contacts with the United States. Apparently a lot of his toys are obtained through United States vendors.

Toys' request for jurisdictional discovery was specific, non-frivolous, and a logical follow-up based on the information known to Toys. The District Court erred by denying this reasonable request. Toys should be allowed jurisdictional discovery, on the limited issue of Step Two's business activities in the United States, including business plans, marketing strategies, sales, and other commercial interactions. Although Step Two does not appear to have widespread contacts with the United States, this limited discovery will also help determine whether jurisdiction exists under the federal long-arm statute. Accordingly, on remand, the District Court should consider whether any newly discovered facts will support jurisdiction under traditional jurisdictional analysis, or under Rule 4(k)(2).

CONCLUSION

For all of the reasons set forth above, we reverse the District Court's denial of Toys' request for jurisdictional discovery, vacate the District Court's dismissal of Toys' complaint, and remand the case for limited jurisdictional discovery guided by the foregoing analysis, and for reconsideration of jurisdiction with the benefit of the product of that discovery.

Specht v. Netscape Communications Corp., 306 F.3d 17 (2d Cir. 2002).
Sotomayor, Circuit Judge.

This is an appeal from a judgment of the Southern District of New York denying a motion by defendants-appellants Netscape Communications Corporation and its corporate parent, America Online, Inc. (collectively, "defendants" or "Netscape"), to compel arbitration and to stay court proceedings. In order to resolve the central question of arbitrability presented here, we must address issues of contract formation in cyberspace. Principally, we are asked to determine whether plaintiffs-appellees ("plaintiffs"), by acting upon defendants' invitation to download free software made available on defendants' webpage, agreed to be bound by the software's license terms (which included the arbitration clause at issue), even though plaintiffs could not have learned of the existence of those terms unless, prior to executing the download, they had scrolled down the webpage to a screen located below the download button. We agree with the district court that a reasonably prudent Internet user in circumstances such as these would not have known or learned of the existence of the license terms before responding to defendants' invitation to download the free software, and that defendants therefore did not provide reasonable notice of the license terms. In consequence, plaintiffs' bare act of downloading the software did not unambiguously manifest assent to the arbitration provision contained in the license terms.

We also agree with the district court that plaintiffs' claims relating to the software at issue—a "plug-in" program entitled SmartDownload ("SmartDownload" or "the plug-in program"), offered by Netscape to enhance the functioning of the separate browser program called Netscape Communicator ("Communicator" or "the browser program")—are not subject to an arbitration agreement contained in the license terms governing the use of Communicator. Finally, we conclude that the district court properly rejected defendants' argument that plaintiff website owner Christopher Specht, though not a party to any Netscape license agreement, is nevertheless required to arbitrate his claims concerning SmartDownload because he allegedly benefited directly under SmartDownload's license agreement. Defendants' theory that Specht benefited whenever visitors employing SmartDownload downloaded certain files made available on his website is simply too tenuous and speculative to justify application of the legal doctrine that requires a nonparty to an arbitration agreement to arbitrate if he or she has received a direct benefit under a contract containing the arbitration agreement.

We therefore affirm the district court's denial of defendants' motion to compel arbitration and to stay court proceedings.

BACKGROUND

I. Facts

In three related putative class actions, plaintiffs alleged that, unknown to them, their use of SmartDownload transmitted to defendants private information about plaintiffs' downloading of files from the Internet, thereby effecting an electronic surveillance of their online activities in violation of two federal statutes, the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 et seq., and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

Specifically, plaintiffs alleged that when they first used Netscape's Communicator—a software program that permits Internet browsing—the program created and stored on each of their computer hard drives a small text file known as a "cookie" that functioned "as a kind of electronic identification tag for future communications" between their computers and Netscape. Plaintiffs further alleged that when they installed SmartDownload—a separate software "plug-in"[2] that served to enhance Communicator's browsing capabilities—SmartDownload created and stored on their computer hard drives another string of characters, known as a "Key," which similarly functioned as an identification tag in future communications with Netscape. According to the complaints in this case, each time a computer user employed Communicator to download a file from the Internet, SmartDownload "assume[d] from Communicator the task of downloading" the file and transmitted to Netscape the address of the file being downloaded together with the cookie created by Communicator and the Key created by SmartDownload. These processes, plaintiffs claim, constituted unlawful "eavesdropping" on users of Netscape's software products as well as on Internet websites from which users employing SmartDownload downloaded files.

In the time period relevant to this litigation, Netscape offered on its website various software programs, including Communicator and SmartDownload, which visitors to the site were invited to obtain free of charge. It is undisputed that five of the six named plaintiffs—Michael Fagan, John Gibson, Mark Gruber, Sean Kelly, and Sherry Weindorf—downloaded Communicator from the Netscape website. These plaintiffs acknowledge that when they proceeded to initiate installation[3] of Communicator, they were automatically shown a scrollable text of that program's license agreement and were not permitted to complete the installation until they had clicked on a "Yes" button to indicate that they accepted all the license terms.[4] If a user attempted to install Communicator without clicking "Yes," the installation would be aborted. All five named user plaintiffs[5] expressly agreed to Communicator's license terms by clicking "Yes." The Communicator license agreement that these plaintiffs saw made no mention of SmartDownload or other plug-in programs, and stated that "[t]hese terms apply to Netscape Communicator and

[2] Netscape's website defines "plug-ins" as "software programs that extend the capabilities of the Netscape Browser in a specific way-giving you, for example, the ability to play audio samples or view video movies from within your browser." SmartDownload purportedly made it easier for users of browser programs like Communicator to download files from the Internet without losing their progress when they paused to engage in some other task, or if their Internet connection was severed.

[3] There is a difference between downloading and installing a software program. When a user downloads a program from the Internet to his or her computer, the program file is stored on the user's hard drive but typically is not operable until the user installs or executes it, usually by double-clicking on the file and causing the program to run.

[4] This kind of online software license agreement has come to be known as "clickwrap" (by analogy to "shrinkwrap," used in the licensing of tangible forms of software sold in packages) because it "presents the user with a message on his or her computer screen, requiring that the user manifest his or her assent to the terms of the license agreement by clicking on an icon. The product cannot be obtained or used unless and until the icon is clicked." Just as breaking the shrinkwrap seal and using the enclosed computer program after encountering notice of the existence of governing license terms has been deemed by some courts to constitute assent to those terms in the context of tangible software, see, e.g., ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1451 (7th Cir. 1996), so clicking on a webpage's clickwrap button after receiving notice of the existence of license terms has been held by some courts to manifest an Internet user's assent to terms governing the use of downloadable intangible software.

[5] The term "user plaintiffs" here and elsewhere in this opinion denotes those plaintiffs who are suing for harm they allegedly incurred as computer users, in contrast to plaintiff Specht, who alleges that he was harmed in his capacity as a website owner.

Netscape Navigator"[6] and that "all disputes relating to this Agreement (excepting any dispute relating to intellectual property rights)" are subject to "binding arbitration in Santa Clara County, California."

Although Communicator could be obtained independently of SmartDownload, all the named user plaintiffs, except Fagan, downloaded and installed Communicator in connection with downloading SmartDownload.[7] Each of these plaintiffs allegedly arrived at a Netscape webpage captioned "SmartDownload Communicator" that urged them to "Download With Confidence Using SmartDownload!" At or near the bottom of the screen facing plaintiffs was the prompt "Start Download" and a tinted button labeled "Download." By clicking on the button, plaintiffs initiated the download of SmartDownload. Once that process was complete, SmartDownload, as its first plug-in task, permitted plaintiffs to proceed with downloading and installing Communicator, an operation that was accompanied by the clickwrap display of Communicator's license terms described above.

The signal difference between downloading Communicator and downloading SmartDownload was that no clickwrap presentation accompanied the latter operation. Instead, once plaintiffs Gibson, Gruber, Kelly, and Weindorf had clicked on the "Download" button located at or near the bottom of their screen, and the downloading of SmartDownload was complete, these plaintiffs encountered no further information about the plug-in program or the existence of license terms governing its use.[9] The sole reference to SmartDownload's license terms on the "SmartDownload Communicator" webpage was located in text that would have become visible to plaintiffs only if they had scrolled down to the next screen.

Had plaintiffs scrolled down instead of acting on defendants' invitation to click on the "Download" button, they would have encountered the following invitation: "Please review and agree to the terms of the Netscape SmartDownload software license agreement before downloading and using the software." Plaintiffs Gibson, Gruber, Kelly, and Weindorf averred in their affidavits that they never saw this reference to the SmartDownload license agreement when they clicked on the "Download" button. They also testified during depositions that they saw no reference to license terms when they clicked to download SmartDownload, although under questioning by defendants' counsel, some plaintiffs added that they could not "remember" or be "sure" whether the screen shots of the SmartDownload page attached to their affidavits reflected precisely what they had seen on their computer screens when they downloaded SmartDownload.

---

[6] While Navigator was Netscape's "stand-alone" Internet browser program during the period in question, Communicator was a "software suite" that comprised Navigator and other software products. All five named user plaintiffs stated in affidavits that they had obtained upgraded versions of Communicator. Fagan, who, as noted below, allegedly did not obtain the browser program in connection with downloading SmartDownload, expressed some uncertainty during his deposition as to whether he had acquired Communicator or Navigator. The identity of Fagan's browser program is immaterial to this appeal, however, as Communicator and Navigator shared the same license agreement.

[7] Unlike the four other user plaintiffs, Fagan chose the option of obtaining Netscape's browser program without first downloading SmartDownload. As discussed below, Fagan allegedly obtained SmartDownload from a separate "shareware" website unrelated to Netscape.

[9] Plaintiff Kelly, a relatively sophisticated Internet user, testified that when he clicked to download SmartDownload, he did not think that he was downloading a software program at all, but rather that SmartDownload "was merely a piece of download technology." He later became aware that SmartDownload was residing as software on his hard drive when he attempted to download electronic files from the Internet.

In sum, plaintiffs Gibson, Gruber, Kelly, and Weindorf allege that the process of obtaining SmartDownload contrasted sharply with that of obtaining Communicator. Having selected SmartDownload, they were required neither to express unambiguous assent to that program's license agreement nor even to view the license terms or become aware of their existence before proceeding with the invited download of the free plug-in program. Moreover, once these plaintiffs had initiated the download, the existence of SmartDownload's license terms was not mentioned while the software was running or at any later point in plaintiffs' experience of the product.

Even for a user who, unlike plaintiffs, did happen to scroll down past the download button, SmartDownload's license terms would not have been immediately displayed in the manner of Communicator's clickwrapped terms. Instead, if such a user had seen the notice of SmartDownload's terms and then clicked on the underlined invitation to review and agree to the terms, a hypertext link would have taken the user to a separate webpage entitled "License & Support Agreements." The first paragraph on this page read, in pertinent part:

> The use of each Netscape software product is governed by a license agreement. You must read and agree to the license agreement terms BEFORE acquiring a product. Please click on the appropriate link below to review the current license agreement for the product of interest to you before acquisition. For products available for download, you must read and agree to the license agreement terms BEFORE you install the software. If you do not agree to the license terms, do not download, install or use the software.

Below this paragraph appeared a list of license agreements, the first of which was " License Agreement for Netscape Navigator and Netscape Communicator Product Family (Netscape Navigator, Netscape Communicator and Netscape SmartDownload)." If the user clicked on that link, he or she would be taken to yet another webpage that contained the full text of a license agreement that was identical in every respect to the Communicator license agreement except that it stated that its "terms apply to Netscape Communicator, Netscape Navigator, and Netscape SmartDownload." The license agreement granted the user a nonexclusive license to use and reproduce the software, subject to certain terms:

> BY CLICKING THE ACCEPTANCE BUTTON OR INSTALLING OR USING NETSCAPE COMMUNICATOR, NETSCAPE NAVIGATOR, OR NETSCAPE SMARTDOWNLOAD SOFTWARE (THE "PRODUCT"), THE INDIVIDUAL OR ENTITY LICENSING THE PRODUCT ("LICENSEE") IS CONSENTING TO BE BOUND BY AND IS BECOMING A PARTY TO THIS AGREEMENT. IF LICENSEE DOES NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, THE BUTTON INDICATING NON-ACCEPTANCE MUST BE SELECTED, AND LICENSEE MUST NOT INSTALL OR USE THE SOFTWARE.

Among the license terms was a provision requiring virtually all disputes relating to the agreement to be submitted to arbitration:

> Unless otherwise agreed in writing, all disputes relating to this Agreement (excepting any dispute relating to intellectual property rights) shall be subject to final and binding arbitration in Santa Clara County, California, under the auspices of JAMS/EndDispute, with the losing party paying all costs of arbitration.

Unlike the four named user plaintiffs who downloaded SmartDownload from the Netscape website, the fifth named plaintiff, Michael Fagan, claims to have downloaded the plug-in program from a "shareware" website operated by ZDNet, an entity unrelated to Netscape. Shareware sites are websites, maintained by companies or individuals, that contain libraries of free, publicly available software. The pages that a user would have seen while downloading SmartDownload from ZDNet differed from those that he or she would have encountered while downloading SmartDownload from the Netscape website. Notably, instead of any kind of notice of the SmartDownload license agreement, the ZDNet pages offered only a hypertext link to "more information" about SmartDownload, which, if clicked on, took the user to a Netscape webpage that, in turn, contained a link to the license agreement. Thus, a visitor to the ZDNet website could have obtained SmartDownload, as Fagan avers he did, without ever seeing a reference to that program's license terms, even if he or she had scrolled through all of ZDNet's webpages.

The sixth named plaintiff, Christopher Specht, never obtained or used SmartDownload, but instead operated a website from which visitors could download certain electronic files that permitted them to create an account with an internet service provider called WhyWeb. Specht alleges that every time a user who had previously installed SmartDownload visited his website and downloaded WhyWeb-related files, defendants intercepted this information. Defendants allege that Specht would receive a representative's commission from WhyWeb every time a user who obtained a WhyWeb file from his website subsequently subscribed to the WhyWeb service. Thus, argue defendants, because the "Netscape license agreement ... conferred on each user the right to download and use both Communicator and SmartDownload software," Specht received a benefit under that license agreement in that SmartDownload "assisted in obtaining the WhyWeb file and increased the likelihood of success in the download process." This benefit, defendants claim, was direct enough to require Specht to arbitrate his claims pursuant to Netscape's license terms. Specht, however, maintains that he never received any commissions based on the WhyWeb files available on his website….

DISCUSSION

I. Standard of Review and Applicable Law…

If a court finds that the parties agreed to arbitrate, it should then consider whether the dispute falls within the scope of the arbitration agreement. A district court's determination of the scope of an arbitration agreement is reviewed de novo. In addition, whether a party may be compelled to arbitrate as a result of direct benefits that he or she allegedly received under a contract entered into by others is an issue of arbitrability that is reviewed de novo.

The FAA provides that a "written provision in any ... contract evidencing a transaction involving commerce to settle by arbitration a controversy thereafter arising out of such contract or transaction ... shall be valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract." It is well settled that a court may not compel arbitration until it has resolved "the question of the very existence" of the contract embodying the arbitration clause. "[A]rbitration is a matter of contract and a party cannot be required to submit to arbitration any dispute which he has not agreed so to submit." Unless the parties clearly provide otherwise, "the question of arbitrability—whether a[n] ... agreement creates a duty for the parties to arbitrate the particular grievance—is undeniably an issue for judicial determination."

The district court properly concluded that in deciding whether parties agreed to arbitrate a certain matter, a court should generally apply state-law principles to the issue of contract formation. Therefore, state law governs the question of whether the parties in the present case entered into an agreement to arbitrate disputes relating to the SmartDownload license agreement. The district court further held that California law governs the question of contract formation here; the parties do not appeal that determination….

III. Whether the User Plaintiffs Had Reasonable Notice of and Manifested Assent to the SmartDownload License Agreement

Whether governed by the common law or by Article 2 of the Uniform Commercial Code ("UCC"), a transaction, in order to be a contract, requires a manifestation of agreement between the parties. See…Cal. Com. Code § 2204(1) ("A contract for sale of goods may be made in any manner sufficient to show agreement, including conduct by both parties which recognizes the existence of such a contract.").[13] Mutual manifestation of assent, whether by written or spoken

[13] The district court concluded that the SmartDownload transactions here should be governed by "California law as it relates to the sale of goods, including the Uniform Commercial Code in effect in California." It is not obvious, however, that UCC Article 2 ("sales of goods") applies to the licensing of software that is downloadable from the Internet. There is no doubt that a sale of tangible goods over the Internet is governed by Article 2 of the UCC. Some courts have also applied Article 2, occasionally with misgivings, to sales of off-the-shelf software in tangible, packaged formats. See, e.g., ProCD, 86 F.3d at 1450 ("[W]e treat the [database] licenses as ordinary contracts accompanying the sale of products, and therefore as governed by the common law of contracts and the Uniform Commercial Code. Whether there are legal differences between 'contracts' and 'licenses' (which may matter under the copyright doctrine of first sale) is a subject for another day."); I.Lan Sys., Inc. v. Nextpoint Networks, Inc., 183 F. Supp. 2d 328, 332 (D. Mass. 2002) (stating, in the context of a dispute between business parties, that "Article 2 technically does not, and certainly will not in the future, govern software licenses, but for the time being, the Court will assume that it does").

Downloadable software, however, is scarcely a "tangible" good, and, in part because software may be obtained, copied, or transferred effortlessly at the stroke of a computer key, licensing of such Internet products has assumed a vast importance in recent years. Recognizing that "a body of law based on images of the sale of manufactured goods ill fits licenses and other transactions in computer information," the National Conference of Commissioners on Uniform State Laws has promulgated the Uniform Computer Information Transactions Act ("UCITA"), a code resembling UCC Article 2 in many respects but drafted to reflect emergent practices in the sale and licensing of computer information. UCITA—originally intended as a new Article 2B to supplement Articles 2 and 2A of the UCC but later proposed as an independent code—has been adopted by two states, Maryland and Virginia.

word or by conduct, is the touchstone of contract…cf. Restatement (Second) of Contracts § 19(2) (1981) ("The conduct of a party is not effective as a manifestation of his assent unless he intends to engage in the conduct and knows or has reason to know that the other party may infer from his conduct that he assents."). Although an onlooker observing the disputed transactions in this case would have seen each of the user plaintiffs click on the SmartDownload "Download" button, see Cedars Sinai Med. Ctr. v. Mid-West Nat'l Life Ins. Co., 118 F. Supp. 2d 1002, 1008 (C.D. Cal. 2000) ("In California, a party's intent to contract is judged objectively, by the party's outward manifestation of consent."), a consumer's clicking on a download button does not communicate assent to contractual terms if the offer did not make clear to the consumer that clicking on the download button would signify assent to those terms, see Windsor Mills, 25 Cal. App. 3d at 992 ("[W]hen the offeree does not know that a proposal has been made to him this objective standard does not apply."). California's common law is clear that "an offeree, regardless of apparent manifestation of his consent, is not bound by inconspicuous contractual provisions of which he is unaware, contained in a document whose contractual nature is not obvious."

Arbitration agreements are no exception to the requirement of manifestation of assent. "This principle of knowing consent applies with particular force to provisions for arbitration." Clarity and conspicuousness of arbitration terms are important in securing informed assent. "If a party wishes to bind in writing another to an agreement to arbitrate future disputes, such purpose should be accomplished in a way that each party to the arrangement will fully and clearly comprehend that the agreement to arbitrate exists and binds the parties thereto." Thus, California contract law measures assent by an objective standard that takes into account both what the offeree said, wrote, or did and the transactional context in which the offeree verbalized or acted.

A. The Reasonably Prudent Offeree of Downloadable Software

Defendants argue that plaintiffs must be held to a standard of reasonable prudence and that, because notice of the existence of SmartDownload license terms was on the next scrollable screen, plaintiffs were on "inquiry notice" of those terms.[14] We disagree with the proposition that a reasonably prudent offeree in plaintiffs' position would necessarily have known or learned of the existence of the SmartDownload license agreement prior to acting, so that plaintiffs may be held to have assented to that agreement with constructive notice of its terms. It is true that "[a] party cannot avoid the terms of a contract on the ground that he or she failed to read it before signing." But courts are quick to add: "An exception to this general rule exists when the writing does not appear to be a contract and the terms are not called to the attention of the recipient. In such a case, no contract is formed with respect to the undisclosed term."

Most of the cases cited by defendants in support of their inquiry-notice argument are drawn from the world of paper contracting. See, e.g., Taussig v. Bode & Haslett, 134 Cal. 260, 66 P. 259 (1901) (where party had opportunity to read leakage disclaimer printed on warehouse receipt, he had duty to do so); In re First Capital Life Ins. Co., 34 Cal. App. 4th 1283, 1288 (1995)

We need not decide today whether UCC Article 2 applies to Internet transactions in downloadable products. The district court's analysis and the parties' arguments on appeal show that, for present purposes, there is no essential difference between UCC Article 2 and the common law of contracts. We therefore apply the common law, with exceptions as noted.

[14] "Inquiry notice" is "actual notice of circumstances sufficient to put a prudent man upon inquiry."

(purchase of insurance policy after opportunity to read and understand policy terms creates binding agreement); King v. Larsen Realty, Inc., 121 Cal. App. 3d 349, 356 (1981) (where realtors' board manual specifying that party was required to arbitrate was "readily available," party was "on notice" that he was agreeing to mandatory arbitration); Cal. State Auto. Ass'n Inter-Ins. Bureau v. Barrett Garages, Inc., 257 Cal. App. 2d 71, 76 (1967) (recipient of airport parking claim check was bound by terms printed on claim check, because a "ordinarily prudent" person would have been alerted to the terms); Larrus v. First Nat'l Bank, 122 Cal. App. 2d 884, 888 (1954) ("clearly printed" statement on bank card stating that depositor agreed to bank's regulations provided sufficient notice to create agreement, where party had opportunity to view statement and to ask for full text of regulations, but did not do so)….

As the foregoing cases suggest, receipt of a physical document containing contract terms or notice thereof is frequently deemed, in the world of paper transactions, a sufficient circumstance to place the offeree on inquiry notice of those terms. "Every person who has actual notice of circumstances sufficient to put a prudent man upon inquiry as to a particular fact, has constructive notice of the fact itself in all cases in which, by prosecuting such inquiry, he might have learned such fact." Cal. Civ. Code § 19. These principles apply equally to the emergent world of online product delivery, pop-up screens, hyperlinked pages, clickwrap licensing, scrollable documents, and urgent admonitions to "Download Now!". What plaintiffs saw when they were being invited by defendants to download this fast, free plug-in called SmartDownload was a screen containing praise for the product and, at the very bottom of the screen, a "Download" button. Defendants argue that under the principles set forth in the cases cited above, a "fair and prudent person using ordinary care" would have been on inquiry notice of SmartDownload's license terms.

We are not persuaded that a reasonably prudent offeree in these circumstances would have known of the existence of license terms. Plaintiffs were responding to an offer that did not carry an immediately visible notice of the existence of license terms or require unambiguous manifestation of assent to those terms. Thus, plaintiffs' "apparent manifestation of ... consent" was to terms "contained in a document whose contractual nature [was] not obvious." Moreover, the fact that, given the position of the scroll bar on their computer screens, plaintiffs may have been aware that an unexplored portion of the Netscape webpage remained below the download button does not mean that they reasonably should have concluded that this portion contained a notice of license terms. In their deposition testimony, plaintiffs variously stated that they used the scroll bar "[o]nly if there is something that I feel I need to see that is on-that is off the page," or that the elevated position of the scroll bar suggested the presence of "mere[ ] formalities, standard lower banner links" or "that the page is bigger than what I can see." Plaintiffs testified, and defendants did not refute, that plaintiffs were in fact unaware that defendants intended to attach license terms to the use of SmartDownload.

We conclude that in circumstances such as these, where consumers are urged to download free software at the immediate click of a button, a reference to the existence of license terms on a submerged screen is not sufficient to place consumers on inquiry or constructive notice of those

terms.[15] The SmartDownload webpage screen was "printed in such a manner that it tended to conceal the fact that it was an express acceptance of [Netscape's] rules and regulations." Internet users may have, as defendants put it, "as much time as they need[ ]" to scroll through multiple screens on a webpage, but there is no reason to assume that viewers will scroll down to subsequent screens simply because screens are there. When products are "free" and users are invited to download them in the absence of reasonably conspicuous notice that they are about to bind themselves to contract terms, the transactional circumstances cannot be fully analogized to those in the paper world of arm's-length bargaining. In the next two sections, we discuss case law and other legal authorities that have addressed the circumstances of computer sales, software licensing, and online transacting. Those authorities tend strongly to support our conclusion that plaintiffs did not manifest assent to SmartDownload's license terms.

B. Shrinkwrap Licensing and Related Practices

Defendants cite certain well-known cases involving shrinkwrap licensing and related commercial practices in support of their contention that plaintiffs became bound by the SmartDownload license terms by virtue of inquiry notice. For example, in Hill v. Gateway 2000, Inc., 105 F.3d 1147 (7th Cir. 1997), the Seventh Circuit held that where a purchaser had ordered a computer over the telephone, received the order in a shipped box containing the computer along with printed contract terms, and did not return the computer within the thirty days required by the terms, the purchaser was bound by the contract. In ProCD, Inc. v. Zeidenberg, the same court held that where an individual purchased software in a box containing license terms which were displayed on the computer screen every time the user executed the software program, the user had sufficient opportunity to review the terms and to return the software, and so was contractually bound after retaining the product. ProCD, 86 F.3d at 1452; cf. Moore v. Microsoft Corp., 293 A.D.2d 587, 587 (2d Dep't 2002) (software user was bound by license agreement where terms were prominently displayed on computer screen before software could be installed and where user was required to indicate assent by clicking "I agree"); Brower v. Gateway 2000, Inc., 246 A.D.2d 246, 251 (1st Dep't 1998) (buyer assented to arbitration clause shipped inside box with computer and software by retaining items beyond date specified by license terms); M.A. Mortenson Co. v. Timberline Software Corp., 93 Wash.App. 819 (1999) (buyer manifested assent to software license terms by installing and using software), aff'd, 140 Wash.2d 568, 998 P.2d 305 (2000); see also I.Lan Sys., 183 F. Supp. 2d at 338 (business entity "explicitly accepted the clickwrap license agreement [contained in purchased software] when it clicked on the box stating 'I agree'").

These cases do not help defendants. To the extent that they hold that the purchaser of a computer or tangible software is contractually bound after failing to object to printed license terms provided with the product, *Hill* and *Brower* do not differ markedly from the cases involving traditional paper contracting discussed in the previous section. Insofar as the purchaser in *ProCD* was confronted with conspicuous, mandatory license terms every time he ran the software on his computer, that case actually undermines defendants' contention that downloading in the absence of conspicuous terms is an act that binds plaintiffs to those terms. In *Mortenson,* the full text of

[15] We do not address the district court's alternative holding that notice was further vitiated by the fact that the reference to SmartDownload's license terms, even if scrolled to, was couched in precatory terms ("a mild request") rather than mandatory ones.

license terms was printed on each sealed diskette envelope inside the software box, printed again on the inside cover of the user manual, and notice of the terms appeared on the computer screen every time the purchaser executed the program. In sum, the foregoing cases are clearly distinguishable from the facts of the present action.

C. Online Transactions

Cases in which courts have found contracts arising from Internet use do not assist defendants, because in those circumstances there was much clearer notice than in the present case that a user's act would manifest assent to contract terms.[16] See, e.g., Hotmail Corp. v. Van$ Money Pie Inc., 47 U.S.P.Q.2d 1020, 1025 (N.D. Cal. 1998) (granting preliminary injunction based in part on breach of "Terms of Service" agreement, to which defendants had assented); America Online, Inc. v. Booker, 781 So.2d 423, 425 (Fla. Dist. Ct. App. 2001) (upholding forum selection clause in "freely negotiated agreement" contained in online terms of service); Caspi v. Microsoft Network, L.L.C., 323 N.J.Super. 118 (N.J.Super.Ct.App.Div. 1999) (upholding forum selection clause where subscribers to online software were required to review license terms in scrollable window and to click "I Agree" or "I Don't Agree"); Barnett v. Network Solutions, Inc., 38 S.W.3d 200, 203-04 (Tex. App. 2001) (upholding forum selection clause in online contract for registering Internet domain names that required users to scroll through terms before accepting or rejecting them); cf. Pollstar v. Gigmania, Ltd., 170 F. Supp. 2d 974, 981-82 (E.D. Cal. 2000) (expressing concern that notice of license terms had appeared in small, gray text on a gray background on a linked webpage, but concluding that it was too early in the case to order dismissal).[17]

---

[16] Defendants place great importance on Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238 (S.D.N.Y. 2000), which held that a user of the Internet domain-name database, Register.com, had "manifested its assent to be bound" by the database's terms of use when it electronically submitted queries to the database. But Verio is not helpful to defendants. There, the plaintiff's terms of use of its information were well known to the defendant, which took the information daily with full awareness that it was using the information in a manner prohibited by the terms of the plaintiff's offer. The case is not closely analogous to ours.

[17] Although the parties here do not refer to it, California's consumer fraud statute, Cal. Bus. & Prof.Code § 17538, is one of the few state statutes to regulate online transactions in goods or services. The statute provides that in disclosing information regarding return and refund policies and other vital consumer information, online vendors must legibly display the information either:

> (i) [on] the first screen displayed when the vendor's electronic site is accessed, (ii) on the screen on which goods or services are first offered, (iii) on the screen on which a buyer may place the order for goods or services, (iv) on the screen on which the buyer may enter payment information, such as a credit card account number, or (v) for nonbrowser-based technologies, in a manner that gives the user a reasonable opportunity to review that information.

The statute's clear purpose is to ensure that consumers engaging in online transactions have relevant information before they can be bound. Although consumer fraud as such is not alleged in the present action, and § 17538 protects only California residents, we note that the statute is consistent with the principle of conspicuous notice of the existence of contract terms that is also found in California's common law of contracts.

In addition, the model code, UCITA, discussed above, generally recognizes the importance of conspicuous notice and unambiguous manifestation of assent in online sales and licensing of computer information. For example, § 112, which addresses manifestation of assent, provides that a user's opportunity to review online contract terms exists if a "record" (or electronic writing) of the contract terms is "made available in a manner that ought to call it to the attention of a reasonable person and permit review." Section 112 also provides, in pertinent part, that "[a] person manifests assent to a record or term if the person, acting with knowledge of, or after having an opportunity to review the record or term or a copy of it ... intentionally engages in conduct or makes statements with reason to know that the other party or its electronic agent may infer from the conduct or statement that the person assents to the record or

After reviewing the California common law and other relevant legal authority, we conclude that under the circumstances here, plaintiffs' downloading of SmartDownload did not constitute acceptance of defendants' license terms. Reasonably conspicuous notice of the existence of contract terms and unambiguous manifestation of assent to those terms by consumers are essential if electronic bargaining is to have integrity and credibility. We hold that a reasonably prudent offeree in plaintiffs' position would not have known or learned, prior to acting on the invitation to download, of the reference to SmartDownload's license terms hidden below the "Download" button on the next screen. We affirm the district court's conclusion that the user plaintiffs, including Fagan, are not bound by the arbitration clause contained in those terms.[18]

IV. Whether Plaintiffs' Assent to Communicator's License Agreement Requires Them To Arbitrate Their Claims Regarding SmartDownload

Plaintiffs do not dispute that they assented to the license terms governing Netscape's Communicator. The parties disagree, however, over the scope of that license's arbitration clause. Defendants contend that the scope is broad enough to encompass plaintiffs' claims regarding SmartDownload, even if plaintiffs did not separately assent to SmartDownload's license terms and even though Communicator's license terms did not expressly mention SmartDownload. Thus, defendants argue, plaintiffs must arbitrate.

---

term." In the case of a "mass-market license," a party adopts the terms of the license only by manifesting assent "before or during the party's initial performance or use of or access to the information."

UCITA § 211 sets forth a number of guidelines for "internet-type" transactions involving the supply of information or software. For example, a licensor should make standard terms "available for review" prior to delivery or obligation to pay (1) by "displaying prominently and in close proximity to a description of the computer information, or to instructions or steps for acquiring it, the standard terms or a reference to an electronic location from which they can be readily obtained," or (2) by "disclosing the availability of the standard terms in a prominent place on the site from which the computer information is offered and promptly furnishing a copy of the standard terms on request before the transfer of the computer information." The commentary to § 211 adds: "The intent of the close proximity standard is that the terms or the reference to them would be called to the attention of an ordinary reasonable person." The commentary also approves of prominent hypertext links that draw attention to the existence of a standard agreement and allow users to view the terms of the license.

We hasten to point out that UCITA, which has been enacted into law only in Maryland and Virginia, does not govern the parties' transactions in the present case, but we nevertheless find that UCITA's provisions offer insight into the evolving online "circumstances" that defendants argue placed plaintiffs on inquiry notice of the existence of the SmartDownload license terms. UCITA has been controversial as a result of the perceived breadth of some of its provisions. Compare Margaret Jane Radin, Humans Computers, and Binding Commitment, 75 Ind. L.J. 1125, 1141 (2000) (arguing that "UCITA's definition of manifestation of assent stretches the ordinary concept of consent"), with Joseph H. Sommer, Against Cyberlaw, 15 Berkeley Tech. L.J. 1145, 1187 (2000) ("There are no new legal developments [in UCITA's assent provisions]. The revolution-if any-occurred with [Karl] Llewellyn's old Article 2, which abandoned most formalisms of contract formation, and sought a contract wherever it could be found."). Nonetheless, UCITA's notice and assent provisions seem to be consistent with well-established principles governing contract formation and enforcement. See Robert A. Hillman & Jeffrey J. Rachlinski, Standard-Form Contracting in the Electronic Age, 77 N.Y.U. L.Rev. 429, 491 (2002) ("[W]e contend that UCITA maintains the contextual, balanced approach to standard terms that can be found in the paper world.").

[18] Because we conclude that the Netscape webpage did not provide reasonable notice of the existence of SmartDownload's license terms, it is irrelevant to our decision whether plaintiff Fagan obtained SmartDownload from that webpage, as defendants contend, or from a shareware website that provided less or no notice of that program's license terms, as Fagan maintains. In either case, Fagan could not be bound by the SmartDownload license agreement….

The scope of an arbitration agreement is a legal issue that we review de novo. "[A]ny doubts concerning the scope of arbitrable issues should be resolved in favor of arbitration." Although "the FAA does not require parties to arbitrate when they have not agreed to do so," arbitration is indicated unless it can be said "with positive assurance" that an arbitration clause is not susceptible to an interpretation that covers the asserted dispute.

The Communicator license agreement, which required arbitration of "all disputes relating to this Agreement (excepting any dispute relating to intellectual property rights)," must be classified as "broad." Where the scope of an arbitration agreement is broad,

> there arises a presumption of arbitrability; if, however, the dispute is in respect of a matter that, on its face, is clearly collateral to the contract, then a court should test the presumption by reviewing the allegations underlying the dispute and by asking whether the claim alleged implicates issues of contract construction or the parties' rights and obligations under it.... [C]laims that present no question involving construction of the contract, and no questions in respect of the parties' rights and obligations under it, are beyond the scope of the arbitration agreement.

In determining whether a particular claim falls within the scope of the parties' arbitration agreement, this Court "focus[es] on the factual allegations in the complaint rather than the legal causes of action asserted." If those allegations "touch matters" covered by the Netscape license agreement, plaintiffs' claims must be arbitrated.

To begin with, we find that the underlying dispute in this case—whether defendants violated plaintiffs' rights under the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act—involves matters that are clearly collateral to the Communicator license agreement. While the SmartDownload license agreement expressly applied "to Netscape Communicator, Netscape Navigator, and Netscape SmartDownload," the Communicator license agreement expressly applied only "to Netscape Communicator and Netscape Navigator." Thus, on its face, the Communicator license agreement governed disputes concerning Netscape's browser programs only, not disputes concerning a plug-in program like SmartDownload. Moreover, Communicator's license terms included a merger or integration clause stating that "[t]his Agreement constitutes the entire agreement between the parties concerning the subject matter hereof." SmartDownload's license terms contained the same clause. Such provisions are recognized by California courts as a means of excluding prior or contemporaneous parol evidence from the scope of a contract. Although the presence of merger clauses is not dispositive here, we note that defendants' express desire to limit the reach of the respective license agreements, combined with the absence of reference to SmartDownload in the Communicator license agreement, suggests that a dispute regarding defendants' allegedly unlawful use of SmartDownload is clearly collateral to the Communicator license agreement.

This conclusion is reinforced by the other terms of the Communicator license agreement, which include a provision describing the non-exclusive nature of the grant and permission to reproduce the software for personal and internal business purposes; restrictions on modification, decompilation, redistribution or other sale or transfer, and removal or alteration of trademarks or

other intellectual property; provisions for the licensor's right to terminate and its proprietary rights; a complete disclaimer of warranties ("as is") and an entire-risk clause; a limitation of liability clause for consequential and other damages, together with a liquidated damages term; clauses regarding encryption and export; a disclaimer of warranties for high risk activities; and a miscellaneous paragraph that contains merger, choice-of-law, arbitration, and severability clauses, non-waiver and non-assignment provisions, a force majeure term, and a clause providing for reimbursement of the prevailing party in any dispute. Apart from the potential generic applicability of the warranty and liability disclaimers, a dispute concerning alleged electronic eavesdropping via transmissions from a separate plug-in program would not appear to fall within Communicator's license terms. We conclude, therefore, that this dispute concerns matters that, on their face, are clearly collateral to the Communicator license agreement.

Having determined this much, we next must test the presumption of arbitrability by asking whether plaintiffs' allegations implicate or touch on issues of contract construction or the parties' rights and obligations under the contract. That is, even though the parties' dispute concerns matters clearly collateral to the Communicator license terms, we must determine whether plaintiffs by their particular allegations have brought the dispute within the license terms. Defendants argue that plaintiffs' complaints "literally bristled with allegations that Communicator and SmartDownload operated in conjunction with one another to eavesdrop on Plaintiffs' Internet communications." We disagree. Plaintiffs' allegations nowhere collapse or blur the distinction between Communicator and SmartDownload, but instead consistently separate the two software programs and assert that SmartDownload alone is responsible for unlawful eavesdropping. Plaintiffs begin by alleging that "SmartDownload facilitates the transfer of large files over the Internet by permitting a transfer to be resumed if it is interrupted." Plaintiffs then explain that "[o]nce SmartDownload is downloaded and running on a Web user's computer, it automatically connects to Netscape's file servers and downloads the installation program for Communicator." Plaintiffs add that defendants also encourage visitors to Netscape's website "to download and install SmartDownload even if they are not installing or upgrading Communicator."

Plaintiffs go on to point out that installing Communicator "automatically creates and stores on the Web user's computer a small text file known as a 'cookie.'" There follow two paragraphs essentially alleging that cookies were originally intended to perform such innocuous tasks as providing "temporary identification for purposes such as electronic commerce," and that the Netscape cookie performs this original identifying, and entirely lawful, function. Separate paragraphs then describe the "Key" or "UserID" that SmartDownload allegedly independently places on user's computers, and point out that "SmartDownload assumes from Communicator the task of downloading various files. Communicator itself could and would perform these downloading tasks if SmartDownload were not installed." "Thereafter," the complaints continue,

> each time a Web user downloads any file from any site on the Internet using SmartDownload, SmartDownload automatically transmits to defendants the name and Internet address of the file and the Web site from which it is being sent. Within the same transmission, SmartDownload also includes the contents of the Netscape cookie previously created by Communicator and the "Key" previously created by SmartDownload.

In the course of their description of the installation and downloading process, plaintiffs keep SmartDownload separate from Communicator and clearly indicate that it is SmartDownload that performed the allegedly unlawful eavesdropping and made use of the otherwise innocuous Communicator cookie as well as its own "Key" and "UserID" to transmit plaintiffs' information to Netscape. The complaints refer to "SmartDownload's spying" and explain that "Defendants are using SmartDownload to eavesdrop." Plaintiffs' allegations consistently distinguish and isolate the functions of SmartDownload in such a way as to make it clear that it is through SmartDownload, not Communicator, that defendants committed the abuses that are the subject of the complaints.

After careful review of these allegations, we conclude that plaintiffs' claims "present no question involving construction of the [Communicator license agreement], and no questions in respect of the parties' rights and obligations under it." It follows that the claims of the five user plaintiffs are beyond the scope of the arbitration clause contained in the Communicator license agreement. Because those claims are not arbitrable under that agreement or under the SmartDownload license agreement, to which plaintiffs never assented, we affirm the district court's holding that the five user plaintiffs may not be compelled to arbitrate their claims….

Register.com, Inc. v. Verio, Inc., 356 F.3d 393 (2d Cir. 2004).
Leval, Circuit Judge.[*]

Defendant, Verio, Inc. ("Verio") appeals from an order of the United States District Court for the Southern District of New York (Barbara S. Jones, J.) granting the motion of plaintiff Register.com, Inc. ("Register") for a preliminary injunction. The court's order enjoined Verio from (1) using Register's trademarks; (2) representing or otherwise suggesting to third parties that Verio's services have the sponsorship, endorsement, or approval of Register; (3) accessing Register's computers by use of automated software programs performing multiple successive queries; and (4) using data obtained from Register's database of contact information of registrants of Internet domain names to solicit the registrants for the sale of web site development services by electronic mail, telephone calls, or direct mail. We affirm.[1]…

BACKGROUND

This plaintiff Register is one of over fifty companies serving as registrars for the issuance of domain names on the world wide web. As a registrar, Register issues domain names to persons and entities preparing to establish web sites on the Internet. Web sites are identified and accessed by reference to their domain names.

Register was appointed a registrar of domain names by the Internet Corporation for Assigned Names and Numbers, known by the acronym "ICANN." ICANN is a private, non-profit public benefit corporation which was established by agencies of the U.S. government to administer the Internet domain name system. To become a registrar of domain names, Register was required to enter into a standard form agreement with ICANN, designated as the ICANN Registrar Accreditation Agreement, November 1999 version (referred to herein as the "ICANN Agreement").

Applicants to register a domain name submit to the registrar contact information, including at a minimum, the applicant's name, postal address, telephone number, and electronic mail address. The ICANN Agreement, referring to this registrant contact information under the rubric "WHOIS information," requires the registrar, under terms discussed in greater detail below, to preserve it, update it daily, and provide for free public access to it through the Internet as well as through an independent access port, called port 43.

[*] The Honorable Fred I. Parker was a member of the panel but died on August 12, 2003. Judge Parker would have voted to reverse the district court's order. This appeal is being decided by the two remaining members of the panel, who are in agreement.

[1] Judge Parker was not in agreement with this disposition. Deliberations have followed an unusual course. Judge Parker initially was assigned to prepare a draft opinion affirming the district court. In the course of preparing the draft, Judge Parker changed his mind and proposed to rule in favor of the defendant, overturning the injunction in most respects. Judge Parker's draft opinion, however, failed to convince the other members of the panel, who adhered to the view that the injunction should be affirmed. Judge Parker died shortly thereafter, prior to the circulation of a draft opinion affirming the injunction, from which Judge Parker presumably would have dissented. [Editor's note: The court attached Judge Parker's draft opinion as an Appendix. It's a scholarly and thoughtful opinion that will reward interested readers.]

Section II.F.5 of the ICANN Agreement (which furnishes a major basis for the appellant Verio's contentions on this appeal) requires that the registrar "not impose terms and conditions" on the use made by others of its WHOIS data "except as permitted by ICANN-adopted policy." In specifying what restrictions may be imposed, the ICANN Agreement requires the registrar to permit use of its WHOIS data "for any lawful purposes except to: ... support the transmission of mass unsolicited, commercial advertising or solicitations *via email* (*spam*); [and other listed purposes not relevant to this appeal]." (emphasis added).

Another section of the ICANN Agreement (upon which appellee Register relies) provides as follows,

> No Third-Party Beneficiaries: This Agreement shall not be construed to create any obligation by either ICANN or Registrar to any non-party to this Agreement ....

Third parties could nonetheless seek enforcement of a registrar's obligations set forth in the ICANN Agreement by resort to a grievance process under ICANN's auspices.

In compliance with § II.F.1 of the ICANN Agreement, Register updated the WHOIS information on a daily basis and established Internet and port 43 service, which allowed free public query of its WHOIS information. An entity making a WHOIS query through Register's Internet site or port 43 would receive a reply furnishing the requested WHOIS information, captioned by a legend devised by Register, which stated,

> By submitting a WHOIS query, you agree that you will use this data only for lawful purposes and that under no circumstances will you use this data to ... support the transmission of mass unsolicited, commercial advertising or solicitation via email.

The terms of that legend tracked § II.F.5 of the ICANN Agreement in specifying the restrictions Register imposed on the use of its WHOIS data. Subsequently, as explained below, Register amended the terms of this legend to impose more stringent restrictions on the use of the information gathered through such queries.

In addition to performing the function of a registrar of domain names, Register also engages in the business of selling web-related services to entities that maintain web sites. These services cover various aspects of web site development. In order to solicit business for the services it offers, Register sends out marketing communications. Among the entities it solicits for the sale of such services are entities whose domain names it registered. However, during the registration process, Register offers registrants the opportunity to elect whether or not they will receive marketing communications from it.

The defendant Verio, against whom the preliminary injunction was issued, is engaged in the business of selling a variety of web site design, development and operation services. In the sale of such services, Verio competes with Register's web site development business. To facilitate its pursuit of customers, Verio undertook to obtain daily updates of the WHOIS information relating

to newly registered domain names. To achieve this, Verio devised an automated software program, or robot, which each day would submit multiple successive WHOIS queries through the port 43 accesses of various registrars. Upon acquiring the WHOIS information of new registrants, Verio would send them marketing solicitations by email, telemarketing and direct mail. To the extent that Verio's solicitations were sent by email, the practice was inconsistent with the terms of the restrictive legend Register attached to its responses to Verio's queries.

At first, Verio's solicitations addressed to Register's registrants made explicit reference to their recent registration through Register. This led some of the recipients of Verio's solicitations to believe the solicitation was initiated by Register (or an affiliate), and was sent in violation of the registrant's election not to receive solicitations from Register. Register began to receive complaints from registrants. Register in turn complained to Verio and demanded that Verio cease and desist from this form of marketing. Register asserted that Verio was harming Register's goodwill, and that by soliciting via email, was violating the terms to which it had agreed on submitting its queries for WHOIS information. Verio responded to the effect that it had stopped mentioning Register in its solicitation message.

In the meantime, Register changed the restrictive legend it attached to its responses to WHOIS queries. While previously the legend conformed to the terms of § II F.5, which authorized Register to prohibit use of the WHOIS information for mass solicitations "via email," its new legend undertook to bar mass solicitation "via direct mail, electronic mail, or by telephone."[2] Section II.F.5 of Register's ICANN Agreement, as noted above, required Register to permit use of the WHOIS data "for any lawful purpose except to ... support the transmission of mass unsolicited solicitations via email (spam)." Thus, by undertaking to prohibit Verio from using the WHOIS information for solicitations "via direct mail ... or by telephone," Register was acting in apparent violation of this term of its ICANN Agreement.

Register wrote to Verio demanding that it cease using WHOIS information derived from Register not only for email marketing, but also for marketing by direct mail and telephone. Verio ceased using the information in email marketing, but refused to stop marketing by direct mail and telephone. [Register then sued Verio in August 2000]….

DISCUSSION

Standard of review and preliminary injunction standard…

(a) Verio's enforcement of the restrictions placed on Register by the ICANN Agreement

Verio conceded that it knew of the restrictions Register placed on the use of the WHOIS data and knew that, by using Register's WHOIS data for direct mail and telemarketing solicitations, it was violating Register's restrictions. Verio's principal argument is that Register was not authorized to forbid Verio from using the data for direct mail and telemarketing solicitation because the

[2] The new legend stated:

> By submitting a WHOIS query, you agree that ... under no circumstances will you use this data to ... support the transmission of mass unsolicited ... advertising or solicitations via direct mail, electronic mail, or by telephone.

ICANN Agreement prohibited Register from imposing any "terms and conditions" on use of WHOIS data, "except as permitted by ICANN-adopted policy," which specified that Register was required to permit "any lawful purpose, except ... mass solicitation[ ] via email."

Register does not deny that the restrictions it imposed contravened this requirement of the ICANN Agreement. Register contends, however, that the question whether it violated § II.F.5 of its Agreement with ICANN is a matter between itself and ICANN, and that Verio cannot enforce the obligations placed on Register by the ICANN Agreement. Register points to § II.S.2 of the ICANN Agreement, captioned "No Third-Party Beneficiaries," which, as noted, states that the agreement is not to be construed "to create any obligation by either ICANN or Registrar to any non-party." Register asserts that Verio, a non-party, is asking the court to construe § II.F.5 as creating an obligation owed by Register to Verio, and that the Agreement expressly forbids such a construction.

ICANN intervened in the district court as an amicus curiae and strongly supports Register's position, opposing Verio's right to invoke Register's contractual promises to ICANN. ICANN explained that ICANN has established a remedial process for the resolution of such disputes through which Verio might have sought satisfaction. "If Verio had concerns regarding Register.com's conditions for access to WHOIS data, it should have raised them within the ICANN process rather [than] simply taking Register.com's data, violating the conditions [imposed by Register], and then seeking to justify its violation in this Court .... [Verio's claim was] intended to be addressed only within the ICANN process."

ICANN asserted that the No Third-Party Beneficiary provision, barring third parties from seeking to enforce promises made by a registrar to ICANN through court proceedings, was "vital to the overall scheme of [its] various agreements."

This is because proper expression of the letter and spirit of ICANN policies is most appropriately achieved through the ICANN process itself, and not through forums that lack the every day familiarity with the intricate technical and policy issues that the ICANN process was designed to address.

ICANN's brief went on to state:

> [E]nforcement of agreements with ICANN [was to] be informed by the judgment of the various segments of the internet community as expressed through ICANN. In the fast-paced environment of the Internet, new issues and situations arise quickly, and sometimes the language of contractual provisions does not perfectly match the underlying policies. For this and other reasons, hard-and-fast enforcement [by courts] of the letter of every term of every agreement is not always appropriate. An integral part of the agreements that the registrars ... entered with ICANN is the understanding that these situations would be handled through consultation and consideration within the ICANN process .... Allowing issues under the agreements registrars make with ICANN to be diverted from [ICANN's] carefully crafted remedial scheme to the courts, at the behest of third parties ..., would seriously threaten the Internet community's ability, under the

> auspices of ICANN, to achieve a proper balance of the competing policy values that are so frequently involved.

We are persuaded by the arguments Register and ICANN advance. It is true Register incurred a contractual obligation to ICANN not to prevent the use of its WHOIS data for direct mail and telemarketing solicitation. But ICANN deliberately included in the same contract that persons aggrieved by Register's violation of such a term should seek satisfaction within the framework of ICANN's grievance policy, and should not be heard in courts of law to plead entitlement to enforce Register's promise to ICANN. As experience develops in the fast changing world of the Internet, ICANN, informed by the various constituencies in the Internet community, might well no longer consider it salutary to enforce a policy which it earlier expressed in the ICANN Agreement. For courts to undertake to enforce promises made by registrars to ICANN at the instance of third parties might therefore be harmful to ICANN's efforts to develop well-informed and sound Internet policy.

Verio's invocation of the ICANN Agreement necessarily depends on its entitlement to enforce Register's promises to ICANN in the role of third party beneficiary. The ICANN Agreement specified that it should be deemed to have been made in California, where ICANN is located. Under § 1559 of the California Civil Code, a "contract, made expressly for the benefit of a third person, may be enforced by him." For Verio to seek to enforce Register's promises it made to ICANN in the ICANN Agreement, Verio must show that the Agreement was made for its benefit. Verio did not meet this burden. To the contrary, the Agreement expressly and intentionally excluded non-parties from claiming rights under it in court proceedings.

We are not persuaded by the arguments Judge Parker advanced in his draft. Although acknowledging that Verio could not claim third party beneficiary rights to enforce Register's promises to ICANN, Judge Parker nonetheless found three reasons for enforcing Verio's claim: (i) "public policy interests at stake," (ii) Register's "indisputable obligations to ICANN as a registrar," and (iii) the equities, involving Register's "unclean hands" in imposing a restriction it was contractually bound not to impose. We respectfully disagree. As for the first argument, that Register's restriction violated public policy, it is far from clear that this is so. It is true that the ICANN Agreement at the time ICANN presented it to Register permitted mass solicitation by means other than email. But it is not clear that at the time of this dispute, ICANN intended to adhere to that policy. As ICANN's amicus brief suggested, the world of the Internet changes rapidly, and public policy as to how that world should be governed may change rapidly as well. ICANN in fact has since changed the terms of its standard agreement for the accreditation of registrars to broaden the uses of WHOIS information that registrars may prohibit to include not only mass email solicitations but also mass telephone and fax solicitations. It is far from clear that ICANN continues to view public policy the way it did at the time it crafted Register's agreement. In any event, if Verio wished to have the dispute resolved in accordance with public policy, it was free to bring its grievance to ICANN. Verio declined to do so. ICANN included the "No Third-Party Beneficiary" provision precisely so that it would retain control of enforcement of policy, rather than yielding it to courts.

As for Judge Parker's second argument, Register's "indisputable obligation to ICANN as a registrar" to permit Verio to use the WHOIS information for mass solicitation by mail and

telephone, we do not see how this argument differs from Verio's claim of entitlement as a third party beneficiary, which § II.S.2 explicitly negates. The fact that Register owed a contractual obligation to ICANN not to impose certain restrictions on use of WHOIS information does not mean that it owed an obligation to Verio not to impose such restrictions. As ICANN's brief in the district court indicates, ICANN was well aware of Register's deviation from the restrictions imposed by the ICANN Agreement, but ICANN chose not to take steps to compel Register to adhere to its contract.

Nor are we convinced by Judge Parker's third argument of Register's "unclean hands." Judge Parker characterizes Register's failure to honor its contractual obligation to ICANN as unethical conduct, making Register ineligible for equitable relief. But Register owed no duty in that regard to anyone but ICANN, and ICANN has expressed no dissatisfaction with Register's failure to adhere to that term of the contract. Verio was free to seek ICANN's intervention on its behalf, but declined to do so, perhaps because it knew or suspected that ICANN would decline to compel Register to adhere to the contract term. Under the circumstances, we see no reason to assume on appeal that Register's conduct should be considered unethical, especially where the district court made no such finding.

(b) Verio's assent to Register's contract terms

Verio's next contention assumes that Register was legally authorized to demand that takers of WHOIS data from its systems refrain from using it for mass solicitation by mail and telephone, as well as by email. Verio contends that it nonetheless never became contractually bound to the conditions imposed by Register's restrictive legend because, in the case of each query Verio made, the legend did not appear until after Verio had submitted the query and received the WHOIS data. Accordingly, Verio contends that in no instance did it receive legally enforceable notice of the conditions Register intended to impose. Verio therefore argues it should not be deemed to have taken WHOIS data from Register's systems subject to Register's conditions.

Verio's argument might well be persuasive if its queries addressed to Register's computers had been sporadic and infrequent. If Verio had submitted only one query, or even if it had submitted only a few sporadic queries, that would give considerable force to its contention that it obtained the WHOIS data without being conscious that Register intended to impose conditions, and without being deemed to have accepted Register's conditions. But Verio was daily submitting numerous queries, each of which resulted in its receiving notice of the terms Register exacted. Furthermore, Verio admits that it knew perfectly well what terms Register demanded. Verio's argument fails.

The situation might be compared to one in which plaintiff P maintains a roadside fruit stand displaying bins of apples. A visitor, defendant D, takes an apple and bites into it. As D turns to leave, D sees a sign, visible only as one turns to exit, which says "Apples—50 cents apiece." D does not pay for the apple. D believes he has no obligation to pay because he had no notice when he bit into the apple that 50 cents was expected in return. D's view is that he never agreed to pay for the apple. Thereafter, each day, several times a day, D revisits the stand, takes an apple, and eats it. D never leaves money.

P sues D in contract for the price of the apples taken. D defends on the ground that on no occasion did he see P's price notice until after he had bitten into the apples. D may well prevail as to the first apple taken. D had no reason to understand upon taking it that P was demanding the payment. In our view, however, D cannot continue on a daily basis to take apples for free, knowing full well that P is offering them only in exchange for 50 cents in compensation, merely because the sign demanding payment is so placed that on each occasion D does not see it until he has bitten into the apple.

Verio's circumstance is effectively the same. Each day Verio repeatedly enters Register's computers and takes that day's new WHOIS data. Each day upon receiving the requested data, Verio receives Register's notice of the terms on which it makes the data available—that the data not be used for mass solicitation via direct mail, email, or telephone. Verio acknowledges that it continued drawing the data from Register's computers with full knowledge that Register offered access subject to these restrictions. Verio is no more free to take Register's data without being bound by the terms on which Register offers it, than D was free, in the example, once he became aware of the terms of P's offer, to take P's apples without obligation to pay the 50 cent price at which P offered them.

Verio seeks support for its position from cases that have dealt with the formation of contracts on the Internet. An excellent example, although decided subsequent to the submission of this case, is Specht v. Netscape Communications Corp., 306 F.3d 17 (2d Cir. 2002). The dispute was whether users of Netscape's software, who downloaded it from Netscape's web site, were bound by an agreement to arbitrate disputes with Netscape, where Netscape had posted the terms of its offer of the software (including the obligation to arbitrate disputes) on the web site from which they downloaded the software. We ruled against Netscape and in favor of the users of its software because the users would not have seen the terms Netscape exacted without scrolling down their computer screens, and there was no reason for them to do so. The evidence did not demonstrate that one who had downloaded Netscape's software had necessarily seen the terms of its offer.

Verio, however, cannot avail itself of the reasoning of Specht. In Specht, the users in whose favor we decided visited Netscape's web site one time to download its software. Netscape's posting of its terms did not compel the conclusion that its downloaders took the software subject to those terms because there was no way to determine that any downloader had seen the terms of the offer. There was no basis for imputing to the downloaders of Netscape's software knowledge of the terms on which the software was offered. This case is crucially different. Verio visited Register's computers daily to access WHOIS data and each day saw the terms of Register's offer; Verio admitted that, in entering Register's computers to get the data, it was fully aware of the terms on which Register offered the access.

Verio's next argument is that it was not bound by Register's terms because it rejected them. Even assuming Register is entitled to demand compliance with its terms in exchange for Verio's entry into its systems to take WHOIS data, and even acknowledging that Verio was fully aware of Register's terms, Verio contends that it still is not bound by Register's terms because it did not agree to be bound. In support of its claim, Verio cites a district court case from the Central District of California, Ticketmaster Corp. v. Tickets.com, Inc., 2000 WL 1887522 (C.D. Cal.

Aug.10, 2000), in which the court rejected Ticketmaster's application for a preliminary injunction to enforce posted terms of use of data available on its website against a regular user. Noting that the user of Ticketmaster's web site is not required to check an "I agree" box before proceeding, the court concluded that there was insufficient proof of agreement to support a preliminary injunction.

We acknowledge that the *Ticketmaster* decision gives Verio some support, but not enough. In the first place, the Ticketmaster court was not making a definitive ruling rejecting Ticketmaster's contract claim. It was rather exercising a district court's discretion to deny a preliminary injunction because of a doubt whether the movant had adequately shown likelihood of success on the merits.

But more importantly, we are not inclined to agree with the Ticketmaster court's analysis. There is a crucial difference between the circumstances of Specht, where we declined to enforce Netscape's specified terms against a user of its software because of inadequate evidence that the user had seen the terms when downloading the software, and those of Ticketmaster, where the taker of information from Ticketmaster's site knew full well the terms on which the information was offered but was not offered an icon marked, "I agree," on which to click. Under the circumstances of Ticketmaster, we see no reason why the enforceability of the offeror's terms should depend on whether the taker states (or clicks), "I agree."

We recognize that contract offers on the Internet often require the offeree to click on an "I agree" icon. And no doubt, in many circumstances, such a statement of agreement by the offeree is essential to the formation of a contract. But not in all circumstances. While new commerce on the Internet has exposed courts to many new situations, it has not fundamentally changed the principles of contract. It is standard contract doctrine that when a benefit is offered subject to stated conditions, and the offeree makes a decision to take the benefit with knowledge of the terms of the offer, the taking constitutes an acceptance of the terms, which accordingly become binding on the offeree. See, e.g., Restatement (Second) of Contracts § 69(1)(a) (1981) ("[S]ilence and inaction operate as an acceptance ... [w]here an offeree takes the benefit of offered services with reasonable opportunity to reject them and reason to know that they were offered with the expectation of compensation."); 2 Richard A. Lord, Williston on Contracts § 6:9 (4th ed. 1991) ("[T]he acceptance of the benefit of services may well be held to imply a promise to pay for them if at the time of acceptance the offeree has a reasonable opportunity to reject the service and knows or has reason to know that compensation is expected."); Arthur Linton Corbin, Corbin on Contracts § 71 (West 1 vol. ed. 1952) ("The acceptance of the benefit of the services is a promise to pay for them, if at the time of accepting the benefit the offeree has a reasonable opportunity to reject it and knows that compensation is expected."); Jones v. Brisbin, 41 Wash.2d 167, 172 (1952) ("Where a person, with reasonable opportunity to reject offered services, takes the benefit of them under circumstances which would indicate, to a reasonable man, that they were offered with the expectation of compensation, a contract, complete with mutual assent, results."); Markstein Bros. Millinery Co. v. J.A. White & Co., 151 Ark. 1 (1921) (buyer of hats was bound to pay for hats when buyer failed to return them to seller within five days of inspection as seller requested in clear and obvious notice statement).

Returning to the apple stand, the visitor, who sees apples offered for 50 cents apiece and takes an apple, owes 50 cents, regardless whether he did or did not say, "I agree." The choice offered in such circumstances is to take the apple on the known terms of the offer or not to take the apple. As we see it, the defendant in Ticketmaster and Verio in this case had a similar choice. Each was offered access to information subject to terms of which they were well aware. Their choice was either to accept the offer of contract, taking the information subject to the terms of the offer, or, if the terms were not acceptable, to decline to take the benefits.

We find that the district court was within its discretion in concluding that Register showed likelihood of success on the merits of its contract claim….

Harris v. Blockbuster Inc., 622 F. Supp. 2d 396 (N.D. Tex. 2009).
Lynn, District Judge.

Background

This case arises out of alleged violations of the Video Privacy Protection Act by Defendant Blockbuster Inc. ("Blockbuster"). Blockbuster operates a service called Blockbuster Online, which allows customers to rent movies through the internet. Blockbuster entered into an agreement with Facebook ("the Blockbuster contract") which caused Blockbuster's customers' movie rental choices to be disseminated on the customers' Facebook accounts through Facebook's "Beacon" program. In short, when a customer rented a video from Blockbuster Online, the Beacon program would transmit the customer's choice to Facebook, which would then broadcast the choice to the customer's Facebook friends.

Plaintiff claims that this arrangement violated the Video Privacy Protection Act, 18 U.S.C. § 2710, which prohibits a videotape service provider from disclosing personally identifiable information about a customer unless given informed, written consent at the time the disclosure is sought. The Act provides for liquidated damages of $2,500 for each violation.

Blockbuster attempted to invoke an arbitration provision in its "Terms and Conditions," which includes a paragraph governing "Dispute Resolution" that states, in pertinent part: "[a]ll claims, disputes or controversies ... will be referred to and determined by binding arbitration." It further purportedly waives the right of its users to commence any class action. As a precondition to joining Blockbuster Online, customers were required to click on a box certifying that they had read and agreed to the Terms and Conditions.

On August 30, 2008, before the case was transferred to this Court, the Defendant moved to enforce the arbitration provision. The Plaintiffs argued that the arbitration provision is unenforceable, principally for two reasons: (1) it is illusory; and (2) it is unconscionable. Because the Court concludes that the arbitration provision is illusory, the Court does not reach the unconscionability issue.

Legal Standard

In Texas, a contract must be supported by consideration, and if it is not, it is illusory and cannot be enforced. In Morrison v. Amway Corp., the Fifth Circuit analyzed a very similar arbitration provision to that in the subject Terms and Conditions and held it to be illusory. In *Morrison*, defendant, a seller of household products marketed through a chain of distributors, was sued by its distributors for a variety of torts, including racketeering and defamation. The defendant sought to enforce an arbitration provision in which each distributor agreed:

> "[T]o conduct [his or her] business according to the Amway Code of Ethics and Rules of Conduct, as they are amended and published from time to time in official Amway literature .... I agree I will give notice in writing of any claim or dispute arising out of or relating to my Amway distributorship, or the Amway Sales and Marketing Plan or Rules of Conduct to the other party or parties .... I agree to

> submit any remaining claim or dispute arising out of or relating to any Amway distributorship, the Amway Sales and Marketing Plan, or the Amway Rules of Conduct ... to binding arbitration in accordance with the Amway Arbitration rules, which are set forth in the Amway Business Compendium."

The *Morrison* court held that the provision was illusory because "[t]here is no express exemption of the arbitration provisions from Amway's ability to unilaterally modify all rules, and the only express limitation on that unilateral right is published notice. While it is inferable that an amendment thus unilaterally made by Amway to the arbitration provision would not become effective until published, there is nothing to suggest that once published the amendment would be inapplicable to disputes arising, or arising out of events occurring, *before* such publication."

The *Morrison* court distinguished In re Halliburton Co., in which the Texas Supreme Court rejected an argument that an arbitration clause was illusory. The provision in Halliburton specifically limited the defendant's ability to apply changes to the agreement as follows:

> [N]o amendment shall apply to a Dispute of which the Sponsor [Halliburton] had actual notice on the date of amendment .... termination [of the arbitration agreement] shall not be effective until 10 days after reasonable notice of termination is given to Employees or as to Disputes which arose prior to the date of termination.

In *Morrison*, the Fifth Circuit held that the limitation on the ability to unilaterally modify or terminate the agreement in *Halliburton* is what caused the Texas Supreme Court to rule that it was enforceable. Because the *Morrison* agreement contained no "*Halliburton* type savings clauses," which would "preclude application of such amendments to disputes which arose (or of which Amway had notice) before the amendment," the agreement in *Morrison* was illusory.

Analysis

The basis for the Plaintiffs' claim that the arbitration provision is illusory is that Blockbuster reserves the right to modify the Terms and Conditions, including the section that contains the arbitration provision, "at its sole discretion" and "at any time," and such modifications will be effective immediately upon being posted on the site. Under the heading "Changes to Terms and Conditions," the contract states:

> Blockbuster may at any time, and at its sole discretion, modify these Terms and Conditions of Use, including without limitation the Privacy Policy, with or without notice. Such modifications will be effective immediately upon posting. You agree to review these Terms and Conditions of Use periodically and your continued use of this Site following such modifications will indicate your acceptance of these modified Terms and Conditions of Use. If you do not agree to any modification of these Terms and Conditions of Use, you must immediately stop using this Site.

The Court concludes that the Blockbuster arbitration provision is illusory for the same reasons as that in *Morrison*. Here, as in *Morrison*, there is nothing in the Terms and Conditions that prevents Blockbuster from unilaterally changing any part of the contract other than providing that such changes will not take effect until posted on the website. There are likewise no "*Halliburton* type savings clauses," as there is "nothing to suggest that once published the amendment would be inapplicable to disputes arising, or arising out of events occurring, before such publication." The Fifth Circuit in *Morrison* noted the lack of an "express exemption" of the ability to unilaterally modify all rules, which the Blockbuster agreement also does not contain. The Blockbuster contract only states that modifications "will be effective immediately upon posting," and the natural reading of that clause does not limit application of the modifications to earlier disputes.

The Court addresses two differences between the Blockbuster contract and that in *Morrison*. Under Texas law, where, as here, an arbitration provision is incorporated within a larger contract, the benefits of the underlying contract can serve as consideration. The *Morrison* contract was a stand-alone agreement, and as such required independent consideration. Second, in *Morrison*, the defendant was actually attempting to retroactively apply the arbitration agreement to events that had happened before it was in effect, and there is no such suggestion here.

Neither distinction affects this Court's determination that the Blockbuster contract is illusory. First, the Supreme Court has broadly held that challenges to a contract as a whole, and not specifically to the arbitration clause, must go to the arbitrator. Defendant argues that because Plaintiffs challenge a provision that applies to the contract as a whole, the challenge must be heard by the arbitrator. The Court disagrees. Plaintiffs' challenge is to the arbitration provision, and therefore the challenge is properly before the Court.

Second, the rule in Morrison applies to cases where there was no attempt to apply a contract modification to prior events. In Simmons v. Quixtar, Inc., the court stated that "a close reading of the Fifth Circuit's opinion [in *Morrison*] is not predicated on that sole ground [of applying modification to earlier actions]. The Court's reasoning applies to the Rules of Conduct and Amway's (Quixtar's) ability to unilaterally change the rules of the game." The court continued: "[t]he language of the Circuit's [*Morrison*] opinion ... decided the issue on the basis that the ability to change the rules at any time made the contract merely illusory." The Court agrees with that analysis and finds that the *Morrison* rule applies even when no retroactive modification has been attempted.

Conclusion

For these reasons, the Court concludes that the arbitration provision of the Blockbuster contract is illusory and unenforceable, and accordingly, Defendant's Motion to Compel Individual Arbitration is denied.

18 U.S.C. §1030: Fraud and related activity in connection with computers
(effective September 26, 2008)

(a) Whoever—
(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y.[(y)] of section 11 of the Atomic Energy Act of 1954 [42 USCS § 2014(y)], with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;
(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
(B) information from any department or agency of the United States; or
(C) information from any protected computer;
(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;
(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $ 5,000 in any 1-year period;
(5) (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.[;]
(6) knowingly and with intent to defraud traffics (as defined in section 1029 [18 USCS § 1029]) in any password or similar information through which a computer may be accessed without authorization, if—
(A) such trafficking affects interstate or foreign commerce; or
(B) such computer is used by or for the Government of the United States; [or]
(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any—
(A) threat to cause damage to a protected computer;

(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;

shall be punished as provided in subsection (c) of this section.

(b) Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is—

(1)

(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section; or an attempt to commit an offense punishable under this subparagraph;

(2) (A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if—

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds $ 5,000; and

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(3)

(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this section;

(4) (A) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 5 years, or both, in the case of—

(i) an offense under subsection (a)(5)(B), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused)—

(I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $ 5,000 in value;

(II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(III) physical injury to any person;

(IV) a threat to public health or safety;

(V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

(VI) damage affecting 10 or more protected computers during any 1-year period; or

(ii) an attempt to commit an offense punishable under this subparagraph;

(B) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 10 years, or both, in the case of—

(i) an offense under subsection (a)(5)(A), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused) a harm provided in subclauses (I) through (VI) of subparagraph (A)(i); or

(ii) an attempt to commit an offense punishable under this subparagraph;

(C) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 20 years, or both, in the case of—

(i) an offense or an attempt to commit an offense under subparagraphs (A) or (B) of subsection (a)(5) that occurs after a conviction for another offense under this section; or

(ii) an attempt to commit an offense punishable under this subparagraph;

(D) a fine under this title, imprisonment for not more than 10 years, or both, in the case of—

(i) an offense or an attempt to commit an offense under subsection (a)(5)(C) that occurs after a conviction for another offense under this section; or

(ii) an attempt to commit an offense punishable under this subparagraph;

(E) if the offender attempts to cause or knowingly or recklessly causes serious bodily injury from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for not more than 20 years, or both;

(F) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both; or

(G) a fine under this title, imprisonment for not more than 1 year, or both, for—

(i) any other offense under subsection (a)(5); or

(ii) an attempt to commit an offense punishable under this subparagraph.

(5) [Deleted]

(d)

(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.

(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title [18 USCS § 3056(a)].

(3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section—

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "protected computer" means a computer—

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;

(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term "financial institution" means—

(A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934 [15 USCS § 78o];

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978 [12 USCS § 3101(1) and (3)]); and

(I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act;

(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

(7) the term “department of the United States” means the legislative or judicial branch of the Government or one of the executive department enumerated in section 101 of title 5;
(8) the term “damage” means any impairment to the integrity or availability of data, a program, a system, or information;
(9) the term “government entity” includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;
(10) the term “conviction” shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;
(11) the term “loss” means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and
(12) the term “person” means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection [enacted Sept. 13, 1994], concerning investigations and prosecutions under subsection (a)(5).

(i) (1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—
(A) such person’s interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation; and
(B) any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violation.
(2) The criminal forfeiture of property under this subsection, any seizure and disposition thereof, and any judicial proceeding in relation thereto, shall be governed by the provisions of

section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

(j) For purposes of subsection (i), the following shall be subject to forfeiture to the United States and no property right shall exist in them:

(1) Any personal property used or intended to be used to commit or to facilitate the commission of any violation of this section, or a conspiracy to violate this section.

(2) Any property, real or personal, which constitutes or is derived from proceeds traceable to any violation of this section, or a conspiracy to violate this section.

California Penal Code Section 502

(a) It is the intent of the Legislature in enacting this section to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems. The Legislature finds and declares that the proliferation of computer technology has resulted in a concomitant proliferation of computer crime and other forms of unauthorized access to computers, computer systems, and computer data.

The Legislature further finds and declares that protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data.

(b) For the purposes of this section, the following terms have the following meanings:
(1) "Access" means to gain entry to, instruct, or communicate with the logical, arithmetical, or memory function resources of a computer, computer system, or computer network.
(2) "Computer network" means any system that provides communications between one or more computer systems and input/output devices including, but not limited to, display terminals and printers connected by telecommunication facilities.
(3) "Computer program or software" means a set of instructions or statements, and related data, that when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions.
(4) "Computer services" includes, but is not limited to, computer time, data processing, or storage functions, or other uses of a computer, computer system, or computer network.
(5) "Computer system" means a device or collection of devices, including support devices and excluding calculators that are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control.
(6) "Data" means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device.
(7) "Supporting documentation" includes, but is not limited to, all information, in any form, pertaining to the design, construction, classification, implementation, use, or modification of a computer, computer system, computer network, computer program, or computer software, which information is not generally available to the public and is necessary for the operation of a computer, computer system, computer network, computer program, or computer software.
(8) "Injury" means any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by the access, or the denial of access to legitimate users of a computer system, network, or program.
(9) "Victim expenditure" means any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, deleted, damaged, or destroyed by the access.

(10) “Computer contaminant” means any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, that are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network.

(11) “Internet domain name” means a globally unique, hierarchical reference to an Internet host or service, assigned through centralized Internet naming authorities, comprising a series of character strings separated by periods, with the rightmost character string specifying the top of the hierarchy.

(c) Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

(9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network.

(d) (1) Any person who violates any of the provisions of paragraph (1), (2), (4), or (5) of subdivision (c) is punishable by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(2) Any person who violates paragraph (3) of subdivision (c) is punishable as follows:

(A) For the first violation that does not result in injury, and where the value of the computer services used does not exceed four hundred dollars ($400), by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(B) For any violation that results in a victim expenditure in an amount greater than five thousand dollars ($5,000) or in an injury, or if the value of the computer services used exceeds four hundred dollars ($400), or for any second or subsequent violation, by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(3) Any person who violates paragraph (6) or (7) of subdivision (c) is punishable as follows:

(A) For a first violation that does not result in injury, an infraction punishable by a fine not exceeding one thousand dollars ($1,000).

(B) For any violation that results in a victim expenditure in an amount not greater than five thousand dollars ($5,000), or for a second or subsequent violation, by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(C) For any violation that results in a victim expenditure in an amount greater than five thousand dollars ($5,000), by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(4) Any person who violates paragraph (8) of subdivision (c) is punishable as follows:

(A) For a first violation that does not result in injury, a misdemeanor punishable by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(B) For any violation that results in injury, or for a second or subsequent violation, by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in a county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment.

(5) Any person who violates paragraph (9) of subdivision (c) is punishable as follows:

(A) For a first violation that does not result in injury, an infraction punishable by a fine not one thousand dollars.

(B) For any violation that results in injury, or for a second or subsequent violation, by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(e) (1) In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief. Compensatory damages shall include any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access. For the purposes of actions authorized by this subdivision, the conduct of an unemancipated minor shall be imputed to the

parent or legal guardian having control or custody of the minor, pursuant to the provisions of Section 1714.1 of the Civil Code.

(2) In any action brought pursuant to this subdivision the court may award reasonable attorney's fees.

(3) A community college, state university, or academic institution accredited in this state is required to include computer-related crimes as a specific violation of college or university student conduct policies and regulations that may subject a student to disciplinary sanctions up to and including dismissal from the academic institution. This paragraph shall not apply to the University of California unless the Board of Regents adopts a resolution to that effect.

(4) In any action brought pursuant to this subdivision for a willful violation of the provisions of subdivision (c), where it is proved by clear and convincing evidence that a defendant has been guilty of oppression, fraud, or malice as defined in subdivision (c) of Section 3294 of the Civil Code, the court may additionally award punitive or exemplary damages.

(5) No action may be brought pursuant to this subdivision unless it is initiated within three years of the date of the act complained of, or the date of the discovery of the damage, whichever is later.

(f) This section shall not be construed to preclude the applicability of any other provision of the criminal law of this state which applies or may apply to any transaction, nor shall it make illegal any employee labor relations activities that are within the scope and protection of state or federal labor laws.

(g) Any computer, computer system, computer network, or any software or data, owned by the defendant, that is used during the commission of any public offense described in subdivision (c) or any computer, owned by the defendant, which is used as a repository for the storage of software or data illegally obtained in violation of subdivision (c) shall be subject to forfeiture, as specified in Section 502.01.

(h) (1) Subdivision (c) does not apply to punish any acts which are committed by a person within the scope of his or her lawful employment. For purposes of this section, a person acts within the scope of his or her employment when he or she performs acts which are reasonably necessary to the performance of his or her work assignment.

(2) Paragraph (3) of subdivision (c) does not apply to penalize any acts committed by a person acting outside of his or her lawful employment, provided that the employee's activities do not cause an injury, as defined in paragraph (8) of subdivision (b), to the employer or another, or provided that the value of supplies or computer services, as defined in paragraph (4) of subdivision (b), which are used does not exceed an accumulated total of one hundred dollars ($100).

(i) No activity exempted from prosecution under paragraph (2) of subdivision (h) which incidentally violates paragraph (2), (4), or (7) of subdivision (c) shall be prosecuted under those paragraphs.

(j) For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one

jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction.

(k) In determining the terms and conditions applicable to a person convicted of a violation of this section the court shall consider the following:

(1) The court shall consider prohibitions on access to and use of computers.

(2) Except as otherwise required by law, the court shall consider alternate sentencing, including community service, if the defendant shows remorse and recognition of the wrongdoing, and an inclination not to repeat the offense.

Comparison of Trespass to Chattels Legal Doctrines

	Chattel Interference	Damage
Restatements (Common law)	intentional use or physical contact	• dispossess • impair condition/quality/value • lost use for substantial time period • bodily harm or harm to legally protected interest
18 USC 1030 (a)(5)(A)	knowingly transmit program/info/code/command	intentionally impair integrity/availability of data, program, system or information without authorization which causes • loss of $5k/yr (includes remediation costs and costs/lost revenues from service interruption) • [medical harm] or physical injury • threat to public health/safety • damage to government computer • damage to 10+ computers/yr
18 USC 1030 (a)(5)(B) & (C)	intentional access without authorization	impair integrity/availability of data, program, system or information which causes • loss of $5k/yr (includes remediation costs and costs/lost revenues from service interruption) • [medical harm] or physical injury • threat to public health/safety • damage to government computer • damage to 10+ computers/yr Note: (B) requires reckless impairment; (C) requires “loss”
CA Penal 502(c)	Knowingly without permission (2) access and take/copy/use data from computer system/network (3) use computer services (7) access computer system/network	any damage or loss (including verification expenses)

Intel Corp. v. Hamidi, 30 Cal.4th 1342 (Cal. 2003).
Werdegar, Justice.

Intel Corporation (Intel) maintains an electronic mail system, connected to the Internet, through which messages between employees and those outside the company can be sent and received, and permits its employees to make reasonable nonbusiness use of this system. On six occasions over almost two years, Kourosh Kenneth Hamidi, a former Intel employee, sent e-mails criticizing Intel's employment practices to numerous current employees on Intel's electronic mail system. Hamidi breached no computer security barriers in order to communicate with Intel employees. He offered to, and did, remove from his mailing list any recipient who so wished. Hamidi's communications to individual Intel employees caused neither physical damage nor functional disruption to the company's computers, nor did they at any time deprive Intel of the use of its computers. The contents of the messages, however, caused discussion among employees and managers.

On these facts, Intel brought suit, claiming that by communicating with its employees over the company's e-mail system Hamidi committed the tort of trespass to chattels. The trial court granted Intel's motion for summary judgment and enjoined Hamidi from any further mailings. A divided Court of Appeal affirmed.

After reviewing the decisions analyzing unauthorized electronic contact with computer systems as potential trespasses to chattels, we conclude that under California law the tort does not encompass, and should not be extended to encompass, an electronic communication that neither damages the recipient computer system nor impairs its functioning. Such an electronic communication does not constitute an actionable trespass to personal property, i.e., the computer system, because it does not interfere with the possessor's use or possession of, or any other legally protected interest in, the personal property itself. The consequential economic damage Intel claims to have suffered, i.e., loss of productivity caused by employees reading and reacting to Hamidi's messages and company efforts to block the messages, is not an injury to the company's interest in its computers—which worked as intended and were unharmed by the communications—any more than the personal distress caused by reading an unpleasant letter would be an injury to the recipient's mailbox, or the loss of privacy caused by an intrusive telephone call would be an injury to the recipient's telephone equipment.

Our conclusion does not rest on any special immunity for communications by electronic mail; we do not hold that messages transmitted through the Internet are exempt from the ordinary rules of tort liability. To the contrary, e-mail, like other forms of communication, may in some circumstances cause legally cognizable injury to the recipient or to third parties and may be actionable under various common law or statutory theories. Indeed, on facts somewhat similar to those here, a company or its employees might be able to plead causes of action for interference with prospective economic relations, interference with contract or intentional infliction of emotional distress. And, of course, as with any other means of publication, third party subjects of e-mail communications may under appropriate facts make claims for defamation, publication of private facts, or other speech-based torts. Intel's claim fails not because e-mail transmitted through the Internet enjoys unique immunity, but because the trespass to chattels tort—unlike the

causes of action just mentioned—may not, in California, be proved without evidence of an injury to the plaintiff's personal property or legal interest therein.

Nor does our holding affect the legal remedies of Internet service providers (ISP's) against senders of unsolicited commercial bulk e-mail (UCE), also known as "spam." A series of federal district court decisions, beginning with CompuServe, Inc. v. Cyber Promotions, Inc. (S.D. Ohio 1997) 962 F. Supp. 1015, has approved the use of trespass to chattels as a theory of spammers' liability to ISP's, based upon evidence that the vast quantities of mail sent by spammers both overburdened the ISP's own computers and made the entire computer system harder to use for recipients, the ISP's customers. In those cases, discussed in greater detail below, the underlying complaint was that the extraordinary quantity of UCE impaired the computer system's functioning. In the present case, the claimed injury is located in the disruption or distraction caused to recipients by the contents of the e-mail messages, an injury entirely separate from, and not directly affecting, the possession or value of personal property.

FACTUAL AND PROCEDURAL BACKGROUND…

Hamidi, a former Intel engineer, together with others, formed an organization named Former and Current Employees of Intel (FACE-Intel) to disseminate information and views critical of Intel's employment and personnel policies and practices. FACE-Intel maintained a Web site (which identified Hamidi as Webmaster and as the organization's spokesperson) containing such material. In addition, over a 21-month period Hamidi, on behalf of FACE-Intel, sent six mass e-mails to employee addresses on Intel's electronic mail system. The messages criticized Intel's employment practices, warned employees of the dangers those practices posed to their careers, suggested employees consider moving to other companies, solicited employees' participation in FACE-Intel, and urged employees to inform themselves further by visiting FACE-Intel's Web site. The messages stated that recipients could, by notifying the sender of their wishes, be removed from FACE-Intel's mailing list; Hamidi did not subsequently send messages to anyone who requested removal.

Each message was sent to thousands of addresses (as many as 35,000 according to FACE-Intel's Web site), though some messages were blocked by Intel before reaching employees. Intel's attempt to block internal transmission of the messages succeeded only in part; Hamidi later admitted he evaded blocking efforts by using different sending computers. When Intel, in March 1998, demanded in writing that Hamidi and FACE-Intel stop sending e-mails to Intel's computer system, Hamidi asserted the organization had a right to communicate with willing Intel employees; he sent a new mass mailing in September 1998.

The summary judgment record contains no evidence Hamidi breached Intel's computer security in order to obtain the recipient addresses for his messages; indeed, internal Intel memoranda show the company's management concluded no security breach had occurred.[1] Hamidi stated he

[1] To the extent, therefore, that Justice Mosk suggests Hamidi breached the security of Intel's internal computer network by "circumvent [ing]" Intel's "security measures" and entering the company's "intranet", the evidence does not support such an implication. An "intranet" is "a network based on TCP/IP protocols (an internet) belonging to an organization, usually a corporation, accessible only by the organization's members, employees, or others with authorization." Hamidi used only a part of Intel's computer network accessible to outsiders.

created the recipient address list using an Intel directory on a floppy disk anonymously sent to him. Nor is there any evidence that the receipt or internal distribution of Hamidi's electronic messages damaged Intel's computer system or slowed or impaired its functioning. Intel did present uncontradicted evidence, however, that many employee recipients asked a company official to stop the messages and that staff time was consumed in attempts to block further messages from FACE-Intel. According to the FACE-Intel Web site, moreover, the messages had prompted discussions between "[e]xcited and nervous managers" and the company's human resources department.

Intel sued Hamidi and FACE-Intel, pleading causes of action for trespass to chattels and nuisance, and seeking both actual damages and an injunction against further e-mail messages. Intel later voluntarily dismissed its nuisance claim and waived its demand for damages. The trial court entered default against FACE-Intel upon that organization's failure to answer. The court then granted Intel's motion for summary judgment, permanently enjoining Hamidi, FACE-Intel, and their agents "from sending unsolicited e-mail to addresses on Intel's computer systems." Hamidi appealed; FACE-Intel did not.

The Court of Appeal, with one justice dissenting, affirmed the grant of injunctive relief. The majority took the view that the use of or intermeddling with another's personal property is actionable as a trespass to chattels without proof of any actual injury to the personal property; even if Intel could not show any damages resulting from Hamidi's sending of messages, "it showed he was disrupting its business by using its property and therefore is entitled to injunctive relief based on a theory of trespass to chattels." The dissenting justice warned that the majority's application of the trespass to chattels tort to "unsolicited electronic mail that causes no harm to the private computer system that receives it" would "expand the tort of trespass to chattel in untold ways and to unanticipated circumstances."…

DISCUSSION

I. Current California Tort Law

Dubbed by Prosser the "little brother of conversion," the tort of trespass to chattels allows recovery for interferences with possession of personal property "not sufficiently important to be classed as conversion, and so to compel the defendant to pay the full value of the thing with which he has interfered."

Though not amounting to conversion, the defendant's interference must, to be actionable, have caused some injury to the chattel or to the plaintiff's rights in it. Under California law, trespass to chattels "lies where an intentional interference with the possession of personal property *has proximately caused injury*." (Thrifty-Tel, Inc. v. Bezenek (1996) 46 Cal. App. 4th 1559, 1566, italics added.) In cases of interference with possession of personal property not amounting to conversion, "the owner has a cause of action for trespass or case, *and may recover only the actual damages suffered by reason of the impairment of the property or the loss of its use*." In modern American law generally, "[t]respass remains as an occasional remedy for minor interferences, *resulting in some damage*, but not sufficiently serious or sufficiently important to

amount to the greater tort" of conversion. (Prosser & Keeton, Torts, supra, § 15, p. 90, italics added.)

The Restatement, too, makes clear that some actual injury must have occurred in order for a trespass to chattels to be actionable. Under section 218 of the Restatement Second of Torts, dispossession alone, without further damages, is actionable, but other forms of interference require some additional harm to the personal property or the possessor's interests in it. "The interest of a possessor of a chattel in its inviolability, unlike the similar interest of a possessor of land, is not given legal protection by an action for nominal damages for harmless intermeddlings with the chattel. In order that an actor who interferes with another's chattel may be liable, his conduct must affect some other and more important interest of the possessor. *Therefore, one who intentionally intermeddles with another's chattel is subject to liability only if his intermeddling is harmful to the possessor's materially valuable interest in the physical condition, quality, or value of the chattel, or if the possessor is deprived of the use of the chattel for a substantial time, or some other legally protected interest of the possessor is affected as stated in Clause (c).* Sufficient legal protection of the possessor's interest in the mere inviolability of his chattel is afforded by his privilege to use reasonable force to protect his possession against even harmless interference."

The Court of Appeal (quoting 7 Speiser et al., American Law of Torts (1990) Trespass, § 23:23, p. 667) referred to "'a number of very early cases [showing that] any unlawful interference, however slight, with the enjoyment by another of his personal property, is a trespass.'" But while a harmless use or touching of personal property may be a technical trespass, an interference (not amounting to dispossession) is not actionable, under modern California and broader American law, without a showing of harm. As already discussed, this is the rule embodied in the Restatement (Rest.2d Torts, § 218) and adopted by California law (Zaslow v. Kroenert, supra, 29 Cal.2d at p. 551; Thrifty-Tel, Inc. v. Bezenek, supra, 46 Cal. App. 4th at p. 1566).

In this respect, as Prosser explains, modern day trespass to chattels differs both from the original English writ and from the action for trespass to land: "Another departure from the original rule of the old writ of trespass concerns the necessity of some actual damage to the chattel before the action can be maintained. Where the defendant merely interferes without doing any harm-as where, for example, he merely lays hands upon the plaintiff's horse, or sits in his car-there has been a division of opinion among the writers, and a surprising dearth of authority. *By analogy to trespass to land there might be a technical tort in such a case .... Such scanty authority as there is, however, has considered that the dignitary interest in the inviolability of chattels, unlike that as to land, is not sufficiently important to require any greater defense than the privilege of using reasonable force when necessary to protect them. Accordingly it has been held that nominal damages will not be awarded, and that in the absence of any actual damage the action will not lie*."

Intel suggests that the requirement of actual harm does not apply here because it sought only injunctive relief, as protection from future injuries. But as Justice Kolkey, dissenting below, observed, "[t]he fact the relief sought is injunctive does not excuse a showing of injury, whether actual or threatened." Indeed, in order to obtain injunctive relief the plaintiff must ordinarily show that the defendant's wrongful acts threaten to cause irreparable injuries, ones that cannot be

adequately compensated in damages. Even in an action for trespass to real property, in which damage to the property is not an element of the cause of action, "the extraordinary remedy of injunction" cannot be invoked without showing the likelihood of irreparable harm. A fortiori, to issue an injunction without a showing of likely irreparable injury in an action for trespass to chattels, in which injury to the personal property or the possessor's interest in it *is* an element of the action, would make little legal sense.

The dispositive issue in this case, therefore, is whether the undisputed facts demonstrate Hamidi's actions caused or threatened to cause damage to Intel's computer system, or injury to its rights in that personal property, such as to entitle Intel to judgment as a matter of law. To review, the undisputed evidence revealed no actual or threatened damage to Intel's computer hardware or software and no interference with its ordinary and intended operation. Intel was not dispossessed of its computers, nor did Hamidi's messages prevent Intel from using its computers for any measurable length of time. Intel presented no evidence its system was slowed or otherwise impaired by the burden of delivering Hamidi's electronic messages. Nor was there any evidence transmission of the messages imposed any marginal cost on the operation of Intel's computers. In sum, no evidence suggested that in sending messages through Intel's Internet connections and internal computer system Hamidi used the system in any manner in which it was not intended to function or impaired the system in any way. Nor does the evidence show the request of any employee to be removed from FACE-Intel's mailing list was not honored. The evidence did show, however, that some employees who found the messages unwelcome asked management to stop them and that Intel technical staff spent time and effort attempting to block the messages. A statement on the FACE-Intel Web site, moreover, could be taken as an admission that the messages had caused "[e]xcited and nervous managers" to discuss the matter with Intel's human resources department.

Relying on a line of decisions, most from federal district courts, applying the tort of trespass to chattels to various types of unwanted electronic contact between computers, Intel contends that, while its computers were not damaged by receiving Hamidi's messages, its interest in the "physical condition, quality or value" of the computers was harmed. We disagree. The cited line of decisions does not persuade us that the mere sending of electronic communications that assertedly cause injury only because of their contents constitutes an actionable trespass to a computer system through which the messages are transmitted. Rather, the decisions finding electronic contact to be a trespass to computer systems have generally involved some actual or threatened interference with the computers' functioning.

In Thrifty-Tel, Inc. v. Bezenek, supra, 46 Cal. App. 4th at pages 1566-1567 (*Thrifty-Tel*), the California Court of Appeal held that evidence of automated searching of a telephone carrier's system for authorization codes supported a cause of action for trespass to chattels. The defendant's automated dialing program "overburdened the [plaintiff's] system, denying some subscribers access to phone lines", showing the requisite injury.

Following *Thrifty-Tel*, a series of federal district court decisions held that sending UCE through an ISP's equipment may constitute trespass to the ISP's computer system. The lead case, CompuServe, Inc. v. Cyber Promotions, Inc., supra, 962 F. Supp. 1015, 1021-1023 (*CompuServe*), was followed by Hotmail Corp. v. Van$ Money Pie, Inc. (N.D. Cal., Apr. 16,

1998) 1998 WL 388389, page *7, America Online, Inc. v. IMS (E.D. Va. 1998) 24 F. Supp. 2d 548, 550-551, and America Online, Inc. v. LCGM, Inc. (E.D. Va. 1998) 46 F. Supp. 2d 444, 451-452.

In each of these spamming cases, the plaintiff showed, or was prepared to show, some interference with the efficient functioning of its computer system. In *CompuServe*, the plaintiff ISP's mail equipment monitor stated that mass UCE mailings, especially from nonexistent addresses such as those used by the defendant, placed "a tremendous burden" on the ISP's equipment, using "disk space and drain[ing] the processing power," making those resources unavailable to serve subscribers. (*CompuServe*, 962 F. Supp. at p. 1022.) Similarly, in Hotmail Corp. v. Van$ Money Pie, Inc., 1998 WL 388389 at page *7, the court found the evidence supported a finding that the defendant's mailings "fill[ed] up Hotmail's computer storage space and threaten [ed] to damage Hotmail's ability to service its legitimate customers." America Online, Inc. v. IMS, decided on summary judgment, was deemed factually indistinguishable from *CompuServe*; the court observed that in both cases the plaintiffs "alleged that processing the bulk e-mail cost them time and money and burdened their equipment." The same court, in America Online, Inc. v. LCGM, Inc., supra, 46 F. Supp. 2d at page 452, simply followed CompuServe and its earlier America Online decision, quoting the former's explanation that UCE burdened the computer's processing power and memory.

Building on the spamming cases, in particular *CompuServe*, three even more recent district court decisions addressed whether unauthorized robotic data collection[4] from a company's publicly accessible Web site is a trespass on the company's computer system. (eBay, Inc. v. Bidder's Edge, Inc., supra, 100 F. Supp. 2d at pp. 1069-1072 (*eBay*); Register.com, Inc. v. Verio, Inc. (S.D.N.Y. 2000) 126 F. Supp. 2d 238, 248-251; Ticketmaster Corp. v. Tickets.com, Inc., supra, 2000 WL 1887522 at p. *4.) The two district courts that found such automated data collection to constitute a trespass relied, in part, on the deleterious impact this activity could have, especially if replicated by other searchers, on the functioning of a Web site's computer equipment.

In the leading case, *eBay*, the defendant Bidder's Edge (BE), operating an auction aggregation site, accessed the eBay Web site about 100,000 times per day, accounting for between 1 and 2 percent of the information requests received by eBay and a slightly smaller percentage of the data transferred by eBay. The district court rejected eBay's claim that it was entitled to injunctive relief because of the defendant's unauthorized presence alone, or because of the incremental cost the defendant had imposed on operation of the eBay site, but found sufficient proof of threatened harm in the potential for others to imitate the defendant's activity: "If BE's activity is allowed to continue unchecked, it would encourage other auction aggregators to engage in similar recursive searching of the eBay system such that eBay would suffer irreparable harm from reduced system performance, system unavailability, or data losses." Again, in addressing the likelihood of eBay's success on its trespass to chattels cause of action, the court held the evidence of injury to eBay's computer system sufficient to support a preliminary injunction: "If the court were to hold otherwise, it would likely encourage other auction aggregators to crawl the eBay site, potentially to the point of denying effective access to eBay's customers. If preliminary injunctive relief were

[4] Data search and collection robots, also known as "Web bots" or "spiders," are programs designed to rapidly search numerous Web pages or sites, collecting, retrieving, and indexing information from these pages. Their uses include creation of searchable databases, Web catalogues and comparison shopping services.

denied, and other aggregators began to crawl the eBay site, there appears to be little doubt that the load on eBay's computer system would qualify as a substantial impairment of condition or value."

Another district court followed *eBay* on similar facts—a domain name registrar's claim against a Web hosting and development site that robotically searched the registrar's database of newly registered domain names in search of business leads—in Register.com, Inc. v. Verio, Inc. Although the plaintiff was unable to measure the burden the defendant's searching had placed on its system, the district court, quoting the declaration of one of the plaintiff's officers, found sufficient evidence of threatened harm to the system in the possibility the defendant's activities would be copied by others: "'I believe that if Verio's searching of Register.com's WHOIS database were determined to be lawful, then every purveyor of Internet-based services would engage in similar conduct.'" Like eBay, the court observed, Register.com had a legitimate fear "that its servers will be flooded by search robots."

In the third decision discussing robotic data collection as a trespass, Ticketmaster Corp. v. Tickets.com, Inc. (*Ticketmaster*), the court, distinguishing eBay, found insufficient evidence of harm to the chattel to constitute an actionable trespass: "A basic element of trespass to chattels must be physical harm to the chattel (not present here) or some obstruction of its basic function (in the court's opinion not sufficiently shown here).... The comparative use [by the defendant of the plaintiff's computer system] appears very small and there is no showing that the use interferes to any extent with the regular business of [the plaintiff].... *Nor here is the specter of dozens or more parasites joining the fray, the cumulative total of which could affect the operation of [the plaintiff's] business*."

In the decisions so far reviewed, the defendant's use of the plaintiff's computer system was held sufficient to support an action for trespass when it actually did, or threatened to, interfere with the intended functioning of the system, as by significantly reducing its available memory and processing power. In *Ticketmaster*, the one case where no such effect, actual or threatened, had been demonstrated, the court found insufficient evidence of harm to support a trespass action. These decisions do not persuade us to Intel's position here, for Intel has demonstrated neither any appreciable effect on the operation of its computer system from Hamidi's messages, nor any likelihood that Hamidi's actions will be replicated by others if found not to constitute a trespass.

That Intel does not claim the type of functional impact that spammers and robots have been alleged to cause is not surprising in light of the differences between Hamidi's activities and those of a commercial enterprise that uses sheer quantity of messages as its communications strategy. Though Hamidi sent thousands of copies of the same message on six occasions over 21 months, that number is minuscule compared to the amounts of mail sent by commercial operations. The individual advertisers sued in America Online, Inc. v. IMS, and America Online, Inc. v. LCGM, Inc., were alleged to have sent more than 60 million messages over 10 months and more than 92 million messages over seven months, respectively. Collectively, UCE has reportedly come to constitute about 45 percent of all e-mail. The functional burden on Intel's computers, or the cost in time to individual recipients, of receiving Hamidi's occasional advocacy messages cannot be compared to the burdens and costs caused ISP's and their customers by the ever-rising deluge of commercial e-mail.

Intel relies on language in the *eBay* decision suggesting that unauthorized use of another's chattel is actionable even without any showing of injury: "Even if, as [defendant] BE argues, its searches use only a small amount of eBay's computer system capacity, BE has nonetheless deprived eBay of the ability to use that portion of its personal property for its own purposes. The law recognizes no such right to use another's personal property." But as the *eBay* court went on immediately to find that the defendant's conduct, if widely replicated, *would* likely impair the functioning of the plaintiff's system, we do not read the quoted remarks as expressing the court's complete view of the issue. In isolation, moreover, they would not be a correct statement of California or general American law on this point. While one may have no *right* temporarily to use another's personal property, such use is actionable as a trespass only if it "has proximately caused injury." (Thrifty-Tel, supra, 46 Cal. App. 4th at p. 1566.) "[I]n the absence of any actual damage the action will not lie." (Prosser & Keeton, Torts, supra, § 14, p. 87.) Short of dispossession, personal injury, or physical damage (not present here), intermeddling is actionable only if "the chattel is impaired as to its condition, quality, or value, or [¶] ... the possessor is deprived of the use of the chattel for a substantial time." (Rest.2d Torts, § 218, pars. (b), (c).) In particular, an actionable deprivation of use "must be for a time so substantial that it is possible to estimate the loss caused thereby. A mere momentary or theoretical deprivation of use is not sufficient unless there is a dispossession...." That Hamidi's messages temporarily used some portion of the Intel computers' processors or storage is, therefore, not enough; Intel must, but does not, demonstrate some measurable loss from the use of its computer system.[5]

In addition to impairment of system functionality, *CompuServe* and its progeny also refer to the ISP's loss of business reputation and customer goodwill, resulting from the inconvenience and cost that spam causes to its members, as harm to the ISP's legally protected interests in its personal property. Intel argues that its own interest in employee productivity, assertedly disrupted by Hamidi's messages, is a comparable protected interest in its computer system. We disagree.

Whether the economic injuries identified in *CompuServe* were properly considered injuries to the ISP's possessory interest in its personal property, the type of property interest the tort is primarily intended to protect, has been questioned.[6] "[T]he court broke the chain between the

---

[5] In the most recent decision relied upon by Intel, Oyster Software, Inc. v. Forms Processing, Inc. (N.D. Cal., Dec. 6, 2001) 2001 WL 1736382, pages *12-*13, a federal magistrate judge incorrectly read *eBay* as establishing, under California law, that mere unauthorized use of another's computer system constitutes an actionable trespass. The plaintiff accused the defendant, a business competitor, of copying the metatags (code describing the contents of a Web site to a search engine) from the plaintiff's Web site, resulting in diversion of potential customers for the plaintiff's services. With regard to the plaintiff's trespass claim (the plaintiff also pleaded causes of action for, inter alia, misappropriation, copyright and trademark infringement), the magistrate judge concluded that eBay imposed no requirement of actual damage and that the defendant's conduct was sufficient to establish a trespass "simply because [it] amounted to 'use' of Plaintiff's computer." But as just explained, we do not read *eBay* as holding that the actual injury requirement may be dispensed with, and such a suggestion would, in any event, be erroneous as a statement of California law.

[6] In support of its reasoning, the *CompuServe* court cited paragraph (d) of section 218 of the Restatement Second of Torts, which refers to harm "to some person or thing in which the possessor has a legally protected interest." As the comment to this paragraph explains, however, it is intended to cover personal injury to the possessor or another person in whom the possessor has a legal interest, or injury to "other chattel or land" in which the possessor of the chattel subject to the trespass has a legal interest. No personal injury was claimed either in *CompuServe* or in the

trespass and the harm, allowing indirect harms to CompuServe's business interests-reputation, customer goodwill, and employee time-to count as harms to the chattel (the server)." (Quilter, The Continuing Expansion of Cyberspace Trespass to Chattels, 17 Berkeley Tech. L.J. at pp. 429-430.) "[T]his move cuts trespass to chattels free from its moorings of dispossession or the equivalent, allowing the court free reign [sic] to hunt for 'impairment.'" (Burk, The Trouble with Trespass (2000) 4 J. Small & Emerging Bus. L. 27, 35.) But even if the loss of goodwill identified in CompuServe were the type of injury that would give rise to a trespass to chattels claim under California law, Intel's position would not follow, for Intel's claimed injury has even less connection to its personal property than did CompuServe's.

CompuServe's customers were annoyed because the system was inundated with unsolicited commercial messages, making its use for personal communication more difficult and costly. Their complaint, which allegedly led some to cancel their CompuServe service, was about *the functioning of CompuServe's electronic mail service*. Intel's workers, in contrast, were allegedly distracted from their work not because of the frequency or quantity of Hamidi's messages, but because of assertions and opinions the messages conveyed. Intel's complaint is thus about *the contents of the messages* rather than the functioning of the company's e-mail system. Even accepting CompuServe's economic injury rationale, therefore, Intel's position represents a further extension of the trespass to chattels tort, fictionally recharacterizing the allegedly injurious effect of a communication's contents on recipients as an impairment to the device which transmitted the message.

This theory of "impairment by content" (Burk, The Trouble with Trespass, 4 J. Small & Emerging Bus. L. at p. 37) threatens to stretch trespass law to cover injuries far afield from the harms to possession the tort evolved to protect. Intel's theory would expand the tort of trespass to chattels to cover virtually any unconsented-to communication that, solely because of its content, is unwelcome to the recipient or intermediate transmitter. As the dissenting justice below explained, "'Damage' of this nature—the distraction of reading or listening to an unsolicited communication—is not within the scope of the injury against which the trespass-to-chattel tort protects, and indeed trivializes it. After all, '[t]he property interest protected by the old action of trespass was that of possession; and this has continued to affect the character of the action.' Reading an e-mail transmitted to equipment designed to receive it, in and of itself, does not affect the possessory interest in the equipment. [¶] Indeed, if a chattel's receipt of an electronic communication constitutes a trespass to that chattel, then not only are unsolicited telephone calls and faxes trespasses to chattel, but unwelcome radio waves and television signals also constitute a trespass to chattel every time the viewer inadvertently sees or hears the unwanted program." We agree. While unwelcome communications, electronic or otherwise, can cause a variety of injuries to economic relations, reputation and emotions, those interests are protected by other branches of tort law; in order to address them, we need not create a fiction of injury to the communication system.

Nor may Intel appropriately assert a property interest in its employees' time. "The Restatement test clearly speaks in the first instance to the impairment of the chattel.... But employees are not chattels (at least not in the legal sense of the term)." (Burk, The Trouble with Trespass, 4 J.

---

case at bar, and neither the lost goodwill in *CompuServe* nor the loss of employee efficiency claimed in the present case is chattel or land.

Small & Emerging Bus. L. at p. 36.) Whatever interest Intel may have in preventing its employees from receiving disruptive communications, it is not an interest in personal property, and trespass to chattels is therefore not an action that will lie to protect it. Nor, finally, can the fact Intel staff spent time attempting to block Hamidi's messages be bootstrapped into an injury to Intel's possessory interest in its computers. To quote, again, from the dissenting opinion in the Court of Appeal: "[I]t is circular to premise the damage element of a tort solely upon the steps taken to prevent the damage. Injury can only be established by the completed tort's consequences, not by the cost of the steps taken to avoid the injury and prevent the tort; otherwise, we can create injury for every supposed tort."

Intel connected its e-mail system to the Internet and permitted its employees to make use of this connection both for business and, to a reasonable extent, for their own purposes. In doing so, the company necessarily contemplated the employees' receipt of unsolicited as well as solicited communications from other companies and individuals. That some communications would, because of their contents, be unwelcome to Intel management was virtually inevitable. Hamidi did nothing but use the e-mail system for its intended purpose—to communicate with employees. The system worked as designed, delivering the messages without any physical or functional harm or disruption. These occasional transmissions cannot reasonably be viewed as impairing the quality or value of Intel's computer system. We conclude, therefore, that Intel has not presented undisputed facts demonstrating an injury to its personal property, or to its legal interest in that property, that support, under California tort law, an action for trespass to chattels.

II. Proposed Extension of California Tort Law

We next consider whether California common law should be extended to cover, as a trespass to chattels, an otherwise harmless electronic communication whose contents are objectionable. We decline to so expand California law. Intel, of course, was not the recipient of Hamidi's messages, but rather the owner and possessor of computer servers used to relay the messages, and it bases this tort action on that ownership and possession. The property rule proposed is a rigid one, under which the sender of an electronic message would be strictly liable to the owner of equipment through which the communication passes—here, Intel—for any consequential injury flowing from the contents of the communication….

…Creating an absolute property right to exclude undesired communications from one's e-mail and Web servers might help force spammers to internalize the costs they impose on ISP's and their customers. But such a property rule might also create substantial new costs, to e-mail and e-commerce users and to society generally, in lost ease and openness of communication and in lost network benefits. In light of the unresolved controversy, we would be acting rashly to adopt a rule treating computer servers as real property for purposes of trespass law.

The Legislature has already adopted detailed regulations governing UCE. (Bus. & Prof. Code, §§ 17538.4, 17538.45) It may see fit in the future also to regulate noncommercial e-mail, such as that sent by Hamidi, or other kinds of unwanted contact between computers on the Internet, such as that alleged in *eBay*. But we are not persuaded that these perceived problems call at present for judicial creation of a rigid property rule of computer server inviolability. We therefore decline to create an exception, covering Hamidi's unwanted electronic messages to Intel

employees, to the general rule that a trespass to chattels is not actionable if it does not involve actual or threatened injury to the personal property or to the possessor's legally protected interest in the personal property. No such injury having been shown on the undisputed facts, Intel was not entitled to summary judgment in its favor.

III. Constitutional Considerations

Because we conclude no trespass to chattels was shown on the summary judgment record, making the injunction improper on common law grounds, we need not address at length the dissenters' constitutional arguments. A few clarifications are nonetheless in order.

Justice Mosk asserts that this case involves only "a private entity seeking to enforce private trespass rights." But the injunction here was issued by a state court. While a private refusal to transmit another's electronic speech generally does not implicate the First Amendment, because no governmental action is involved (see Cyber Promotions, Inc. v. American Online, Inc. (E.D. Penn. 1996) 948 F. Supp. 436, 441-445 [spammer could not force private ISP to carry its messages]), the use of government power, whether in enforcement of a statute or ordinance or by an award of damages or an injunction in a private lawsuit, is state action that must comply with First Amendment limits. Nor does the nonexistence of a "constitutional right to trespass" make an injunction in this case per se valid. Unlike, for example, the trespasser-to-land defendant in Church of Christ in Hollywood v. Superior Court (2002) 99 Cal. App. 4th 1244, Hamidi himself had no tangible presence on Intel property, instead speaking from his own home through his computer. He no more invaded Intel's property than does a protester holding a sign or shouting through a bullhorn outside corporate headquarters, posting a letter through the mail, or telephoning to complain of a corporate practice.

Justice Brown relies upon a constitutional "right not to listen," rooted in the listener's "personal autonomy", as compelling a remedy against Hamidi's messages, which she asserts were sent to "unwilling" listeners. Even assuming a corporate entity could under some circumstances claim such a personal right, here the intended and actual recipients of Hamidi's messages were individual Intel employees, rather than Intel itself. The record contains no evidence Hamidi sent messages to any employee who notified him such messages were unwelcome. In any event, such evidence would, under the dissent's rationale of a right not to listen, support only a narrow injunction aimed at protecting individual recipients who gave notice of their rejection. (See Bolger v. Youngs Drug Products Corp. (1983) 463 U.S. 60, 72 [government may not act on behalf of all addressees by generally prohibiting mailing of materials related to contraception, where those recipients who may be offended can simply ignore and discard the materials]; Martin v. City of Struthers (1943) 319 U.S. 141, 144 [anti-canvassing ordinance improperly "substitutes the judgment of the community for the judgment of the individual householder"]; cf. Rowan v. U.S. Post Office Dept. (1970) 397 U.S. 728, 736 ["householder" may exercise "individual autonomy" by refusing delivery of offensive mail].) The principle of a right not to listen, founded in personal autonomy, cannot justify the sweeping injunction issued here against all communication to Intel addresses, for such a right, logically, can be exercised only by, or at the behest of, the recipient himself or herself.

DISPOSITION

The judgment of the Court of Appeal is reversed.

WE CONCUR: KENNARD, MORENO and PERREN[*], JJ.

[Concurring opinion by Justice Kennard and dissenting opinion by Justice Brown are omitted.]

Dissenting Opinion by MOSK, J.[**]

The majority hold that the California tort of trespass to chattels does not encompass the use of expressly unwanted electronic mail that causes no physical damage or impairment to the recipient's computer system. They also conclude that because a computer system is not like real property, the rules of trespass to real property are also inapplicable to the circumstances in this case. Finally, they suggest that an injunction to preclude mass, noncommercial, unwelcome e-mails may offend the interests of free communication.

I respectfully disagree and would affirm the trial court's decision. In my view, the repeated transmission of bulk e-mails by appellant Kourosh Kenneth Hamidi (Hamidi) to the employees of Intel Corporation (Intel) on its proprietary confidential e-mail lists, despite Intel's demand that he cease such activities, constituted an actionable trespass to chattels. The majority fail to distinguish open communication in the public "commons" of the Internet from unauthorized intermeddling on a private, proprietary intranet. Hamidi is not communicating in the equivalent of a town square or of an unsolicited "junk" mailing through the United States Postal Service. His action, in crossing from the public Internet into a private intranet, is more like intruding into a private office mailroom, commandeering the mail cart, and dropping off unwanted broadsides on 30,000 desks. Because Intel's security measures have been circumvented by Hamidi, the majority leave Intel, which has exercised all reasonable self-help efforts, with no recourse unless he causes a malfunction or systems "crash." Hamidi's repeated intrusions did more than merely "prompt[ ] discussions between '[e]xcited and nervous managers' and the company's human resource department"; they also constituted a misappropriation of Intel's private computer system contrary to its intended use and against Intel's wishes.

The law of trespass to chattels has not universally been limited to physical damage. I believe it is entirely consistent to apply that legal theory to these circumstances—that is, when a proprietary computer system is being used contrary to its owner's purposes and expressed desires, and self-help has been ineffective. Intel correctly expects protection from an intruder who misuses its proprietary system, its nonpublic directories, and its supposedly controlled connection to the Internet to achieve his bulk mailing objectives—incidentally, without even having to pay postage.

I

[*] Associate Justice of the Court of Appeal, Second Appellate District, Division Six, assigned by the Chief Justice pursuant to article VI, section 6 of the California Constitution.

[**] Associate Justice, Court of Appeal, Second Appellate District, Division Five, assigned by the Chief Justice pursuant to article VI, section 6 of the California Constitution

Intel maintains an intranet—a proprietary computer network—as a tool for transacting and managing its business, both internally and for external business communications.[1] The network and its servers constitute a tangible entity that has value in terms of the costs of its components and its function in enabling and enhancing the productivity and efficiency of Intel's business operations. Intel has established costly security measures to protect the integrity of its system, including policies about use, proprietary internal e-mail addresses that it does not release to the public for use outside of company business, and a gateway for blocking unwanted electronic mail-a so-called firewall.

The Intel computer usage guidelines, which are promulgated for its employees, state that the computer system is to be "used as a resource in conducting business. Reasonable personal use is permitted, but employees are reminded that these resources are the property of Intel and all information on these resources is also the property of Intel." Examples of personal use that would not be considered reasonable expressly include "use that adversely affects productivity." Employee e-mail communications are neither private nor confidential.

Hamidi, a former Intel employee who had sued Intel and created an organization to disseminate negative information about its employment practices, sent bulk electronic mail on six occasions to as many as 35,000 Intel employees on its proprietary computer system, using Intel's confidential employee e-mail lists and adopting a series of different origination addresses and encoding strategies to elude Intel's blocking efforts. He refused to stop when requested by Intel to do so, asserting that he would ignore its demands: "I don't care. I have grown deaf." Intel sought injunctive relief, alleging that the disruptive effect of the bulk electronic mail, including expenses from administrative and management personnel, damaged its interest in the proprietary nature of its network.

The trial court, in its order granting summary judgment and a permanent injunction, made the following pertinent findings regarding Hamidi's transmission of bulk electronic mail: "Intel has requested that Hamidi stop sending the messages, but Hamidi has refused, and has employed surreptitious means to circumvent Intel's efforts to block entry of his messages into Intel's system.... [¶] ... The e-mail system is dedicated for use in conducting business, including communications between Intel employees and its customers and vendors. Employee e-mail addresses are not published for use outside company business.... [¶] The intrusion by Hamidi into the Intel e-mail system has resulted in the expenditure of company resources to seek to block his mailings and to address employee concerns about the mailings. Given Hamidi's evasive techniques to avoid blocking, the self help remedy available to Intel is ineffective." The trial court concluded that "the evidence establishes (without dispute) that Intel has been injured by diminished employee productivity and in devoting company resources to blocking efforts and to

[1] The Oxford English Dictionary defines an intranet as "A local or restricted computer network; *spec*. a private or corporate network that uses Internet protocols. An intranet may (but need not) be connected to the Internet and be accessible externally to authorized users." (OED Online, new ed., draft entry, Mar. 2003, <http://dictionary.oed.com/> [as of June 30, 2003]; see also Kokka, Property Rights on an Intranet, 3 Spring 1998 J. Tech.L. & Policy 3, WL 3 UFLJTLP 3 at *3, *6 [defining an intranet as "an internal network of computers, servers, routers and browser software designed to organize, secure, distribute and collect information within an organization," which in large organizations generally includes a wide range of services, including e-mail].) Contrary to the majority's assertion, there is nothing incorrect about characterizing Hamidi's unauthorized bulk e-mails as intrusions onto Intel's intranet.

addressing employees about Hamidi's e-mails." The trial court further found that the "massive" intrusions "impaired the value to Intel of its e-mail system."

The majority agree that an impairment of Intel's system would result in an action for trespass to chattels, but find that Intel suffered no injury. As did the trial court, I conclude that the undisputed evidence establishes that Intel was substantially harmed by the costs of efforts to block the messages and diminished employee productivity. Additionally, the injunction did not affect Hamidi's ability to communicate with Intel employees by other means; he apparently continues to maintain a Web site to publicize his messages concerning the company. Furthermore, I believe that the trial court and the Court of Appeal correctly determined that the tort of trespass to chattels applies in these circumstances.

The Restatement Second of Torts explains that a trespass to a chattel occurs if "the chattel is impaired as to its *condition, quality, or value*" or if "harm is caused to some ... thing in which the possessor has a legally protected interest." (Rest.2d Torts, § 218, subds. (b) & (d), p. 420, italics added.) As to this tort, a current prominent treatise on the law of torts explains that "[t]he defendant may interfere with the chattel by interfering with the plaintiff's access or use" and observes that the tort has been applied so as "to protect computer systems from electronic invasions by way of unsolicited email or the like." (1 Dobbs, The Law of Torts (2001) § 60, pp. 122-123.) Moreover, "[t]he harm necessary to trigger liability for trespass to chattels can be ... harm to something other than the chattel itself." (Id., pp. 124-125; see also 1 Harper et al., The Law of Torts (3d ed. 1996 & 2003 supp.) § 2.3, pp. 2:14-2:18.) The Restatement points out that, unlike a possessor of land, a possessor of a chattel is not given legal protection from harmless invasion, but "the actor" may be liable if the conduct affects "some other and more important *interest* of the possessor." (Rest.2d Torts, § 218, com. (e), p. 421, italics added.)

The Restatement explains that the rationale for requiring harm for trespass to a chattel but not for trespass to land is the availability and effectiveness of self-help in the case of trespass to a chattel. "Sufficient legal protection of the possessor's interest in the mere inviolability of his chattel is afforded by his privilege to use reasonable force to protect his possession against even harmless interference." (Rest.2d Torts, § 218, com. (e), p. 422.) Obviously, "force" is not available to prevent electronic trespasses. As shown by Intel's inability to prevent Hamidi's intrusions, self-help is not an adequate alternative to injunctive relief.

The common law tort of trespass to chattels does not require physical disruption to the chattel. It also may apply when there is impairment to the "quality" or "value" of the chattel. (Rest.2d Torts, § 218, subd. (b), p. 420; see also id., com. (e), pp. 421-422 [liability if "intermeddling is harmful to the possessor's materially valuable interest in the physical condition, quality, or value of the chattel"].) Moreover, as we held in Zaslow v. Kroenert (1946) 29 Cal.2d 541, 551, it also applies "[w]here the conduct complained of does not amount to a substantial interference with possession or the right thereto, but consists of intermeddling with or use of or damages to the personal property."[2]

[2] In *Zaslow*, we observed that when the trespass involves "intermeddling with or use of" another's property, the owner "may recover only the actual damages suffered by reason of the impairment of the property or the loss of its use." (Zaslow v. Kroenert, supra, 29 Cal.2d at p. 551) We did not state that such damages were a requirement for a cause of action; nor did we address the availability of injunctive relief.

Here, Hamidi's deliberate and continued intermeddling, and threatened intermeddling, with Intel's proprietary computer system for his own purposes that were hostile to Intel, certainly impaired the quality and value of the system as an internal business device for Intel and forced Intel to incur costs to try to maintain the security and integrity of its server—efforts that proved ineffective. These included costs incurred to mitigate injuries that had already occurred. It is not a matter of "bootstrapp[ing]" to consider those costs a damage to Intel. Indeed, part of the value of the proprietary computer system is the ability to exclude intermeddlers from entering it for significant uses that are disruptive to its owner's business operations.

If Intel, a large business with thousands of former employees, is unable to prevent Hamidi from continued intermeddling, it is not unlikely that other outsiders who obtain access to its proprietary electronic mail addresses would engage in similar conduct, further reducing the value of, and perhaps debilitating, the computer system as a business productivity mechanism. Employees understand that a firewall is in place and expect that the messages they receive are from senders permitted by the corporation. Violation of this expectation increases the internal disruption caused by messages that circumvent the company's attempt to exclude them. The time that each employee must spend to evaluate, delete or respond to the message, when added up, constitutes an amount of compensated time that translates to quantifiable financial damage.[3]

All of these costs to protect the integrity of the computer system and to deal with the disruptive effects of the transmissions and the expenditures attributable to employee time, constitute damages sufficient to establish the existence of a trespass to chattels, even if the computer system was not overburdened to the point of a "crash" by the bulk electronic mail.

The several courts that have applied the tort of trespass to chattels to deliberate intermeddling with proprietary computer systems have, for the most part, used a similar analysis. Thus, the court in CompuServe Inc. v. Cyber Promotions, Inc. (S.D. Ohio 1997) 962 F. Supp. 1015, 1022, applied the Restatement to conclude that mass mailings and evasion of the server's filters diminished the value of the mail processing computer equipment to CompuServe "even though it is not physically damaged by defendant's conduct." The inconvenience to users of the system as a result of the mass messages "decrease[d] the utility of CompuServe's e-mail service" and was actionable as a trespass to chattels. (Id. at p. 1023.)

---

[3] As the recent spate of articles on "spam"—unsolicited bulk e-mail—suggests, the effects on business of such unwanted intrusions are not trivial. "Spam is not just a nuisance. It absorbs bandwidth and overwhelms Internet service providers. Corporate tech staffs labor to deploy filtering technology to protect their networks. The cost is now widely estimated (though all such estimates are largely guesswork) at billions of dollars a year. The social costs are immeasurable.... [¶] 'Spam has become the organized crime of the Internet.' ... '[M]ore and more it's becoming a systems and engineering and networking problem.'" (Gleick, Tangled Up in Spam, N.Y. Times (Feb. 9, 2003) magazine p. 1 [as of June 30, 2003]; see also Cooper & Shogren, U.S., States Turn Focus to Curbing Spam, L.A. Times (May 1, 2003) p. A21, col. 2 ["Businesses are losing money with every moment that employees spend deleting"]; Turley, Congress Must Send Spammers a Message, L.A. Times (Apr. 21, 2003) p. B13, col. 5 ["Spam now costs American businesses about $9 billion a year in lost productivity and screening"]; Taylor, Spam's Big Bang! (June 16, 2003) Time, p. 51 ["The time we spend deleting or defeating spam costs an estimated $8.9 billion a year in lost productivity"].) But the occasional spam addressed to particular employees does not pose nearly the same threat of impaired value as the concerted bulk mailings into one e-mail system at issue here, which mailings were sent to thousands of employees with the express purpose of disrupting business as usual.

The court in America Online, Inc. v. IMS (E.D. Va. 1998) 24 F. Supp. 2d 548, on facts similar to those in the present case, also applied the Restatement in a trespass to chattels claim. There, defendant sent unauthorized e-mails to America Online's computer system, persisting after receiving notice to desist and causing the company "to spend technical resources and staff time to 'defend' its computer system and its membership" against the unwanted messages. The company was not required to show that its computer system was overwhelmed or suffered a diminution in performance; mere use of the system by the defendant was sufficient to allow the plaintiff to prevail on the trespass to chattels claim.

Similarly, the court in eBay, Inc. v. Bidder's Edge, Inc. (N.D. Cal. 2000) 100 F. Supp. 2d 1058 determined that there was a trespass to chattels when the quality or value of a computer system was diminished by unauthorized "web crawlers,"[4] despite the fact that eBay had not alleged any "particular service disruption" or "specific incremental damages" to the computer system. Intermeddling with eBay's private property was sufficient to establish a cause of action: "A trespasser is liable when the trespass diminishes the condition, quality or value of personal property"; "[e]ven if [defendant's intrusions] use only a small amount of eBay's computer ... capacity, [defendant] has nonetheless deprived eBay of the ability to use that portion of its personal property for its own purposes. The law recognizes no such right to use another's personal property." ([S]ee also, e.g., Oyster Software, Inc. v. Forms Processing, Inc. (N.D. Cal., Dec. 6, 200) 2001 WL 1736382 at *12-*13 [trespass to chattels claim did not require company to demonstrate physical damage]; accord, Register.com, Inc. v. Verio, Inc. (S.D.N.Y. 2000) 126 F. Supp. 2d 238, 250; cf. Thrifty-Tel, Inc. v. Bezenek (1996) 46 Cal. App. 4th 1559, 1566-1567 [unconsented electronic access to a computer system constituted a trespass to chattels].)

These cases stand for the simple proposition that owners of computer systems, like owners of other private property, have a right to prevent others from using their property against their interests. That principle applies equally in this case. By his repeated intermeddling, Hamidi converted Intel's private employee e-mail system into a tool for harming productivity and disrupting Intel's workplace. Intel attempted to put a stop to Hamidi's intrusions by increasing its electronic screening measures and by requesting that he desist. Only when self-help proved futile, devolving into a potentially endless joust between attempted prevention and circumvention, did Intel request and obtain equitable relief in the form of an injunction to prevent further threatened injury.

The majority suggest that Intel is not entitled to injunctive relief because it chose to allow its employees access to e-mail through the Internet and because Hamidi has apparently told employees that he will remove them from his mailing list if they so request. They overlook the proprietary nature of Intel's intranet system; Intel's system is not merely a conduit for messages to its employees. As the owner of the computer system, it is Intel's request that Hamidi stop that must be respected. The fact that, like most large businesses, Intel's intranet includes external e-mail access for essential business purposes does not logically mean, as the majority suggest, that Intel has forfeited the right to determine who has access to its system. Its intranet is not the equivalent of a common carrier or public communications licensee that would be subject to requirements to provide service and access. Just as Intel can, and does, regulate the use of its

[4] A "web crawler" is a computer program that operates across the Internet to obtain information from the websites of others.

computer system by its employees, it should be entitled to control its use by outsiders and to seek injunctive relief when self-help fails.

The majority also propose that Intel has sufficient avenues for legal relief outside of trespass to chattels, such as interference with prospective economic relations, interference with contract, intentional infliction of emotional distress, and defamation; Hamidi urges that an action for nuisance is more appropriate. Although other causes of action may under certain circumstances also apply to Hamidi's conduct, the remedy based on trespass to chattels is the most efficient and appropriate. It simply requires Hamidi to stop the unauthorized use of property without regard to the content of the transmissions. Unlike trespass to chattels, the other potential causes of action suggested by the majority and Hamidi would require an evaluation of the transmissions' content and, in the case of a nuisance action, for example, would involve questions of degree and value judgments based on competing interests.

II

As discussed above, I believe that existing legal principles are adequate to support Intel's request for injunctive relief. But even if the injunction in this case amounts to an extension of the traditional tort of trespass to chattels, this is one of those cases in which, as Justice Cardozo suggested, "[t]he creative element in the judicial process finds its opportunity and power" in the development of the law.

The law has evolved to meet economic, social, and scientific changes in society. The industrial revolution, mass production, and new transportation and communication systems all required the adaptation and evolution of legal doctrines.

The age of computer technology and cyberspace poses new challenges to legal principles. As this court has said, "the so-called Internet revolution has spawned a host of new legal issues as courts have struggled to apply traditional legal frameworks to this new communication medium." The court must now grapple with proprietary interests, privacy, and expression arising out of computer-related disputes. Thus, in this case the court is faced with "that balancing of judgment, that testing and sorting of considerations of analogy and logic and utility and fairness" that Justice Cardozo said he had "been trying to describe." Additionally, this is a case in which equitable relief is sought. As Bernard Witkin has written, "equitable relief is flexible and expanding, and the theory that 'for every wrong there is a remedy' [Civ.Code, § 3523] may be invoked by equity courts to justify the invention of new methods of relief for new types of wrongs." That the Legislature has dealt with some aspects of commercial unsolicited bulk e-mail (Bus. & Prof. Code, §§ 17538.4, 17538.45) should not inhibit the application of common law tort principles to deal with e-mail transgressions not covered by the legislation.

Before the computer, a person could not easily cause significant disruption to another's business or personal affairs through methods of communication without significant cost. With the computer, by a mass mailing, one person can at no cost disrupt, damage, and interfere with another's property, business, and personal interests. Here, the law should allow Intel to protect its computer-related property from the unauthorized, harmful, free use by intruders.

III

As the Court of Appeal observed, connecting one's driveway to the general system of roads does not invite demonstrators to use the property as a public forum. Not mindful of this precept, the majority blur the distinction between public and private computer networks in the interest of "ease and openness of communication." By upholding Intel's right to exercise self-help to restrict Hamidi's bulk e-mails, they concede that he did not have a right to send them through Intel's proprietary system. Yet they conclude that injunctive relief is unavailable to Intel because it connected its e-mail system to the Internet and thus, "necessarily contemplated" unsolicited communications to its employees. Their exposition promotes unpredictability in a manner that could be as harmful to open communication as it is to property rights. It permits Intel to block Hamidi's e-mails entirely, but offers no recourse if he succeeds in breaking through its security barriers, unless he physically or functionally degrades the system.

By making more concrete damages a requirement for a remedy, the majority has rendered speech interests dependent on the impact of the e-mails. The sender will never know when or if the mass e-mails sent by him (and perhaps others) will use up too much space or cause a crash in the recipient system, so as to fulfill the majority's requirement of damages. Thus, the sender is exposed to the risk of liability because of the possibility of damages. If, as the majority suggest, such a risk will deter "ease and openness of communication", the majority's formulation does not eliminate such deterrence. Under the majority's position, the lost freedom of communication still exists. In addition, a business could never reliably invest in a private network that can only be kept private by constant vigilance and inventiveness, or by simply shutting off the Internet, thus limiting rather than expanding the flow of information.[6] Moreover, Intel would have less incentive to allow employees reasonable use of its equipment to send and receive personal e-mails if such allowance is justification for preventing restrictions on unwanted intrusions into its computer system. I believe the best approach is to clearly delineate private from public networks and identify as a trespass to chattels the kind of intermeddling involved here.

The views of the amici curiae group of intellectual property professors that a ruling in favor of Intel will interfere with communication are similarly misplaced because here, Intel, contrary to most users, expressly informed Hamidi that it did not want him sending messages through its system. Moreover, as noted above, all of the problems referred to will exist under the apparently accepted law that there is a cause of action if there is some actionable damage.

Hamidi and other amici curiae raise, for the first time on appeal, certain labor law issues, including the matter of protected labor-related communications. Even assuming that these issues are properly before this court, to the extent the laws allow what would otherwise be trespasses for some labor-related communications, my position does not exclude that here too. But there has been no showing that the communications are labor-law protected.[7]

---

[6] Thus, the majority's approach creates the perverse incentive for companies to invest less in computer capacity in order to protect its property. In the view of the majority, Hamidi's massive e-mails would be actionable only if Intel had insufficient server or storage capacity to manage them.

[7] The bulk e-mail messages from Hamidi, a nonemployee, did not purport to spur employees into any collective action; he has conceded that "[t]his is not a drive to unionize." Nor was his disruptive conduct part of any bona fide labor dispute.

Finally, with regard to alleged constitutional free speech concerns raised by Hamidi and others, this case involves a private entity seeking to enforce private rights against trespass. Unlike the majority, I have concluded that Hamidi did invade Intel's property. His actions constituted a trespass—in this case a trespass to chattels. There is no federal or state constitutional right to trespass. (Adderley v. Florida (1966) 385 U.S. 39, 47 ["Nothing in the Constitution of the United States prevents Florida from even-handed enforcement of its general trespass statute...."]; Church of Christ in Hollywood v. Superior Court (2002) 99 Cal. App. 4th 1244, 1253-1254 [affirming a restraining order preventing former church member from entering church property: "[the United States Supreme Court] has never held that a trespasser or an uninvited guest may exercise general rights of free speech on property privately owned"]; see also CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. at p. 1026 ["the mere judicial enforcement of neutral trespass laws by the private owner of property does not alone render it a state actor"]; Cyber Promotions, Inc. v. American Online, Inc. (E.D. Pa. 1996) 948 F. Supp. 436, 456 ["a private company such as Cyber simply does not have the unfettered right under the First Amendment to invade AOL's private property...."].) Accordingly, the cases cited by the majority regarding restrictions on speech, not trespass, are not applicable. Nor does the connection of Intel's e-mail system to the Internet transform it into a public forum any more than any connection between private and public properties. Moreover, as noted above, Hamidi had adequate alternative means for communicating with Intel employees so that an injunction would not, under any theory, constitute a free speech violation.

IV

The trial court granted an injunction to prevent threatened injury to Intel. That is the purpose of an injunction. Intel should not be helpless in the face of repeated and threatened abuse and contamination of its private computer system. The undisputed facts, in my view, rendered Hamidi's conduct legally actionable. Thus, the trial court's decision to grant a permanent injunction was not "a clear abuse of discretion" that may be "disturbed on appeal."

The injunction issued by the trial court simply required Hamidi to refrain from further trespassory conduct, drawing no distinction based on the content of his e-mails. Hamidi remains free to communicate with Intel employees and others outside the walls—both physical and electronic—of the company.

For these reasons, I respectfully dissent.

I CONCUR: GEORGE, C.J.

Register.com, Inc. v. Verio, Inc., 356 F.3d 393 (2d Cir. 2004).
Leval, Circuit Judge.

…Verio also attacks the grant of the preliminary injunction against its accessing Register's computers by automated software programs performing multiple successive queries. This prong of the injunction was premised on Register's claim of trespass to chattels. Verio contends the ruling was in error because Register failed to establish that Verio's conduct resulted in harm to Register's servers and because Verio's robot access to the WHOIS database through Register was "not unauthorized." We believe the district court's findings were within the range of its permissible discretion.

"A trespass to a chattel may be committed by intentionally ... using or intermeddling with a chattel in the possession of another," Restatement (Second) of Torts § 217(b) (1965), where "the chattel is impaired as to its condition, quality, or value."

The district court found that Verio's use of search robots, consisting of software programs performing multiple automated successive queries, consumed a significant portion of the capacity of Register's computer systems. While Verio's robots alone would not incapacitate Register's systems, the court found that if Verio were permitted to continue to access Register's computers through such robots, it was "highly probable" that other Internet service providers would devise similar programs to access Register's data, and that the system would be overtaxed and would crash. We cannot say these findings were unreasonable.

Nor is there merit to Verio's contention that it cannot be engaged in trespass when Register had never instructed it not to use its robot programs. As the district court noted, Register's complaint sufficiently advised Verio that its use of robots was not authorized and, according to Register's contentions, would cause harm to Register's systems….

Copyright Basics, Copyright Office Circular 1 (from http://www.copyright.gov/circs/circ1.pdf) (accessed July 6, 2010)

What Is Copyright?

Copyright is a form of protection provided by the laws of the United States (title 17, U. S. Code) to the authors of "original works of authorship," including literary, dramatic, musical, artistic, and certain other intellectual works. This protection is available to both published and unpublished works. Section 106 of the 1976 Copyright Act generally gives the owner of copyright the exclusive right to do and to authorize others to do the following:

• To reproduce the work in copies or phonorecords;
• To prepare derivative works based upon the work;
• To distribute copies or phonorecords of the work to the public by sale or other transfer of ownership, or by rental, lease, or lending;
• To perform the work publicly, in the case of literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures and other audiovisual works;
• To display the work publicly, in the case of literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work; and
• In the case of sound recordings,[*] to perform the work publicly by means of a digital audio transmission.

In addition, certain authors of works of visual art have the rights of attribution and integrity as described in section 106A of the 1976 Copyright Act….

It is illegal for anyone to violate any of the rights provided by the copyright law to the owner of copyright. These rights, however, are not unlimited in scope. Sections 107 through 121 of the 1976 Copyright Act establish limitations on these rights. In some cases, these limitations are specified exemptions from copyright liability. One major limitation is the doctrine of "fair use," which is given a statutory basis in section 107 of the 1976 Copyright Act. In other instances, the limitation takes the form of a "compulsory license" under which certain limited uses of copyrighted works are permitted upon payment of specified royalties and compliance with statutory conditions….

Who Can Claim Copyright?

Copyright protection subsists from the time the work is created in fixed form. The copyright in the work of authorship immediately becomes the property of the author who created the work. Only the author or those deriving their rights through the author can rightfully claim copyright.

[*] Sound recordings are defined in the law as "works that result from the fixation of a series of musical, spoken, or other sounds, but not including the sounds accompanying a motion picture or other audiovisual work." Common examples include recordings of music, drama, or lectures. A sound recording is not the same as a phonorecord. A phonorecord is the physical object in which works of authorship are embodied. The word "phonorecord" includes cassette tapes, CDs, and vinyl disks as well as other formats.

In the case of works made for hire, the employer and not the employee is considered to be the author. Section 101 of the copyright law defines a “work made for hire” as:
1) a work prepared by an employee within the scope of his or her employment; or
2) a work specially ordered or commissioned for use as:
• a contribution to a collective work
• a part of a motion picture or other audiovisual work
• a translation
• a supplementary work
• a compilation
• an instructional text
• a test
• answer material for a test
• an atlas
if the parties expressly agree in a written instrument signed by them that the work shall be considered a work made for hire.

The authors of a joint work are co-owners of the copyright in the work, unless there is an agreement to the contrary.

Copyright in each separate contribution to a periodical or other collective work is distinct from copyright in the collective work as a whole and vests initially with the author of the contribution.

Two General Principles

• Mere ownership of a book, manuscript, painting, or any other copy or phonorecord does not give the possessor the copyright. The law provides that transfer of ownership of any material object that embodies a protected work does not of itself convey any rights in the copyright.

• Minors may claim copyright, but state laws may regulate the business dealings involving copyrights owned by minors….

What Works Are Protected?

Copyright protects “original works of authorship” that are fixed in a tangible form of expression. The fixation need not be directly perceptible so long as it may be communicated with the aid of a machine or device. Copyrightable works include the following categories:

1) literary works
2) musical works, including any accompanying words
3) dramatic works, including any accompanying music
4) pantomimes and choreographic works
5) pictorial, graphic, and sculptural works
6) motion pictures and other audiovisual works
7) sound recordings
8) architectural works

These categories should be viewed broadly. For example, computer programs and most "compilations" may be registered as "literary works"; maps and architectural plans may be registered as "pictorial, graphic, and sculptural works."

What Is Not Protected by Copyright?

Several categories of material are generally not eligible for federal copyright protection. These include among others:

• Works that have not been fixed in a tangible form of expression (for example, choreographic works that have not been notated or recorded, or improvisational speeches or performances that have not been written or recorded)

• Titles, names, short phrases, and slogans; familiar symbols or designs; mere variations of typographic ornamentation, lettering, or coloring; mere listings of ingredients or contents

• Ideas, procedures, methods, systems, processes, concepts, principles, discoveries, or devices, as distinguished from a description, explanation, or illustration

• Works consisting entirely of information that is common property and containing no original authorship (for example: standard calendars, height and weight charts, tape measures and rulers, and lists or tables taken from public documents or other common sources)

How to Secure a Copyright

Copyright Secured Automatically upon Creation

The way in which copyright protection is secured is frequently misunderstood. No publication or registration or other action in the Copyright Office is required to secure copyright. There are, however, certain definite advantages to registration.

Copyright is secured automatically when the work is created, and a work is "created" when it is fixed in a copy or phonorecord for the first time. "Copies" are material objects from which a work can be read or visually perceived either directly or with the aid of a machine or device, such as books, manuscripts, sheet music, film, videotape, or microfilm. "Phonorecords" are material objects embodying fixations of sounds (excluding, by statutory definition, motion picture soundtracks), such as cassette tapes, CDs, or vinyl disks. Thus, for example, a song (the "work") can be fixed in sheet music ("copies") or in phonograph disks ("phonorecords"), or both. If a work is prepared over a period of time, the part of the work that is fixed on a particular date constitutes the created work as of that date.

Publication

Publication is no longer the key to obtaining federal copyright as it was under the Copyright Act of 1909. However, publication remains important to copyright owners.

The 1976 Copyright Act defines publication as follows:

> "Publication" is the distribution of copies or phonorecords of a work to the public by sale or other transfer of ownership, or by rental, lease, or lending. The offering to distribute copies or phonorecords to a group of persons for purposes of further distribution, public performance, or public display constitutes publication. A public performance or display of a work does not of itself constitute publication.
>
> *Note*: Before 1978, federal copyright was generally secured by the act of publication with notice of copyright, assuming compliance with all other relevant statutory conditions. U. S. works in the public domain on January 1, 1978, (for example, works published without satisfying all conditions for securing federal copyright under the Copyright Act of 1909) remain in the public domain under the 1976 Copyright Act….
>
> Federal copyright could also be secured before 1978 by the act of registration in the case of certain unpublished works and works eligible for ad interim copyright. The 1976 Copyright Act automatically extends to full term (section 304 sets the term) copyright for all works, including those subject to ad interim copyright if ad interim registration has been made on or before June 30, 1978.

A further discussion of the definition of "publication" can be found in the legislative history of the 1976 Copyright Act. The legislative reports define "to the public" as distribution to persons under no explicit or implicit restrictions with respect to disclosure of the contents. The reports state that the definition makes it clear that the sale of phonorecords constitutes publication of the underlying work, for example, the musical, dramatic, or literary work embodied in a phonorecord. The reports also state that it is clear that any form of dissemination in which the material object does not change hands, for example, performances or displays on television, is not a publication no matter how many people are exposed to the work. However, when copies or phonorecords are offered for sale or lease to a group of wholesalers, broadcasters, or motion picture theaters, publication does take place if the purpose is further distribution, public performance,or public display.

Publication is an important concept in the copyright law for several reasons:

• Works that are published in the United States are subject to mandatory deposit with the Library of Congress….
• Publication of a work can affect the limitations on the exclusive rights of the copyright owner that are set forth in sections 107 through 121 of the law.
• The year of publication may determine the duration of copyright protection for anonymous and pseudonymous works (when the author's identity is not revealed in the records of the Copyright Office) and for works made for hire.
• Deposit requirements for registration of published works differ from those for registration of unpublished works….

• When a work is published, it may bear a notice of copyright to identify the year of publication and the name of the copyright owner and to inform the public that the work is protected by copyright. Copies of works published before March 1, 1989, must bear the notice or risk loss of copyright protection….

Notice of Copyright

The use of a copyright notice is no longer required under U. S. law, although it is often beneficial. Because prior law did contain such a requirement, however, the use of notice is still relevant to the copyright status of older works.

Notice was required under the 1976 Copyright Act. This requirement was eliminated when the United States adhered to the Berne Convention, effective March 1, 1989….

The Copyright Office does not take a position on whether copies of works first published with notice before March 1, 1989, which are distributed on or after March 1, 1989, must bear the copyright notice.

Use of the notice may be important because it informs the public that the work is protected by copyright, identifies the copyright owner, and shows the year of first publication. Furthermore, in the event that a work is infringed, if a proper notice of copyright appears on the published copy or copies to which a defendant in a copyright infringement suit had access, then no weight shall be given to such a defendant's interposition of a defense based on innocent infringement in mitigation of actual or statutory damages, except as provided in section 504(c)(2) of the copyright law. Innocent infringement occurs when the infringer did not realize that the work was protected.

The use of the copyright notice is the responsibility of the copyright owner and does not require advance permission from, or registration with, the Copyright Office.

Form of Notice for Visually Perceptible Copies

The notice for visually perceptible copies should contain all the following three elements:

1) The symbol © (the letter C in a circle), or the word "Copyright," or the abbreviation "Copr."; and
2) The year of first publication of the work. In the case of compilations or derivative works incorporating previously published material, the year date of first publication of the compilation or derivative work is sufficient. The year date may be omitted where a pictorial, graphic, or sculptural work, with accompanying textual matter, if any, is reproduced in or on greeting cards, postcards, stationery, jewelry, dolls, toys, or any useful article; and
3) The name of the owner of copyright in the work, or an abbreviation by which the name can be recognized, or a generally known alternative designation of the owner.

Example: © 2008 John Doe….

How Long Copyright Protection Endures

Works Originally Created on or after January 1, 1978

A work that was created (fixed in tangible form for the first time) on or after January 1, 1978, is automatically protected from the moment of its creation and is ordinarily given a term enduring for the author's life plus an additional 70 years after the author's death. In the case of "a joint work prepared by two or more authors who did not work for hire," the term lasts for 70 years after the last surviving author's death. For works made for hire, and for anonymous and pseudonymous works (unless the author's identity is revealed in Copyright Office records), the duration of copyright will be 95 years from publication or 120 years from creation, whichever is shorter….

Transfer of Copyright

Any or all of the copyright owner's exclusive rights or any subdivision of those rights may be transferred, but the transfer of exclusive rights is not valid unless that transfer is in writing and signed by the owner of the rights conveyed or such owner's duly authorized agent. Transfer of a right on a nonexclusive basis does not require a written agreement. A copyright may also be conveyed by operation of law and may be bequeathed by will or pass as personal property by the applicable laws of intestate succession.

Copyright is a personal property right, and it is subject to the various state laws and regulations that govern the ownership, inheritance, or transfer of personal property as well as terms of contracts or conduct of business….

The law does provide for the recordation in the Copyright Office of transfers of copyright ownership. Although recordation is not required to make a valid transfer between the parties, it does provide certain legal advantages and may be required to validate the transfer as against third parties….

Termination of Transfers

Under the previous law, the copyright in a work reverted to the author, if living, or if the author was not living, to other specified beneficiaries, provided a renewal claim was registered in the 28th year of the original term. The present law drops the renewal feature except for works already in the first term of statutory protection when the present law took effect. Instead, the present law permits termination of a grant of rights after 35 years under certain conditions by serving written notice on the transferee within specified time limits….

International Copyright Protection

There is no such thing as an "international copyright" that will automatically protect an author's writings throughout the entire world. Protection against unauthorized use in a particular country depends, basically, on the national laws of that country. However, most countries do offer

protection to foreign works under certain conditions, and these conditions have been greatly simplified by international copyright treaties and conventions….

Copyright Registration

In general, copyright registration is a legal formality intended to make a public record of the basic facts of a particular copyright. However, registration is not a condition of copyright protection. Even though registration is not a requirement for protection, the copyright law provides several inducements or advantages to encourage copyright owners to make registration. Among these advantages are the following:

• Registration establishes a public record of the copyright claim.
• Before an infringement suit may be filed in court, registration is necessary for works of U. S. origin.
• If made before or within five years of publication, registration will establish prima facie evidence in court of the validity of the copyright and of the facts stated in the certificate.
• If registration is made within three months after publication of the work or prior to an infringement of the work, statutory damages and attorney's fees will be available to the copyright owner in court actions. Otherwise, only an award of actual damages and profits is available to the copyright owner.
• Registration allows the owner of the copyright to record the registration with the U. S. Customs Service for protection against the importation of infringing copies….

Registration may be made at any time within the life of the copyright. Unlike the law before 1978, when a work has been registered in unpublished form, it is not necessary to make another registration when the work becomes published, although the copyright owner may register the published edition, if desired….

Fair Use Summary

First Factor (Nature of Use)

Spectrum of commercial to educational uses, where commercial uses are less fair and educational uses are more fair. Some courts treat commercial uses as presumptively unfair (Sony), but Campbell rejected this presumption.

Courts will also consider if the use is transformative or just redistributive. Transformative uses "add something new, with a further purpose or different character, altering the first with new expression, meaning or message" (Campbell). Rarely, courts do not require adding something new if the use has a different purpose (Kelly v. Arriba, but compare Texaco). Transformative uses are more likely to be fair use, and the other three factors are less important (Campbell).

Second Factor (Nature of Work).

Spectrum of fact to fiction, where taking factual works is more fair and taking fiction is less fair. Some courts deem taking unpublished works presumptively unfair (Harper & Row), but §107 was amended to supersede this presumption.

Some courts treat fact/fiction and published/unpublished as two separate sub-factors.

Third Factor (Amount/Substantiality of Portion Taken).

Some courts say that taking the entire work is presumptively unfair. Taking the "heart of the work," even if a small amount, usually isn't fair.

Fourth Factor (Market Effect).

The fourth factor is routinely characterized as the most important factor (Harper & Row). The factor evaluates (1) whether unrestricted and widespread conduct like the defendant's would substantively and adversely impact the market, and (2) the harm to the market for derivative works when these derivative markets are "traditional, reasonable, or likely to be developed markets" (Texaco), but some courts give the copyright owner the option not to pursue a market (Castle Rock). Increasing demand for the underlying work doesn't mitigate harm to a derivative market (Harper & Row; Napster).

Cartoon Network LP, LLLP v. CSC Holdings, Inc., 536 F.3d 121 (2d Cir. 2008)
Walker, Jr., Circuit Judge.

Defendant-Appellant Cablevision Systems Corporation ("Cablevision") wants to market a new "Remote Storage" Digital Video Recorder system ("RS-DVR"), using a technology akin to both traditional, set-top digital video recorders, like TiVo ("DVRs"), and the video-on-demand ("VOD") services provided by many cable companies. Plaintiffs-Appellees produce copyrighted movies and television programs that they provide to Cablevision pursuant to numerous licensing agreements. They contend that Cablevision, through the operation of its RS-DVR system as proposed, would directly infringe their copyrights both by making unauthorized reproductions, and by engaging in public performances, of their copyrighted works. The material facts are not in dispute. Because we conclude that Cablevision would not directly infringe plaintiffs' rights under the Copyright Act by offering its RS-DVR system to consumers, we reverse the district court's award of summary judgment to plaintiffs, and we vacate its injunction against Cablevision.

BACKGROUND

Today's television viewers increasingly use digital video recorders ("DVRs") instead of video cassette recorders ("VCRs") to record television programs and play them back later at their convenience. DVRs generally store recorded programming on an internal hard drive rather than a cassette. But, as this case demonstrates, the generic term "DVR" actually refers to a growing number of different devices and systems. Companies like TiVo sell a stand-alone DVR device that is typically connected to a user's cable box and television much like a VCR. Many cable companies also lease to their subscribers "set-top storage DVRs," which combine many of the functions of a standard cable box and a stand-alone DVR in a single device.

In March 2006, Cablevision, an operator of cable television systems, announced the advent of its new "Remote Storage DVR System." As designed, the RS-DVR allows Cablevision customers who do not have a stand-alone DVR to record cable programming on central hard drives housed and maintained by Cablevision at a "remote" location. RS-DVR customers may then receive playback of those programs through their home television sets, using only a remote control and a standard cable box equipped with the RS-DVR software. Cablevision notified its content providers, including plaintiffs, of its plans to offer RS-DVR, but it did not seek any license from them to operate or sell the RS-DVR.

Plaintiffs, which hold the copyrights to numerous movies and television programs, sued Cablevision for declaratory and injunctive relief. They alleged that Cablevision's proposed operation of the RS-DVR would directly infringe their exclusive rights to both reproduce and publicly perform their copyrighted works. Critically for our analysis here, plaintiffs alleged theories only of direct infringement, not contributory infringement, and defendants waived any defense based on fair use.

Ultimately, the United States District Court for the Southern District of New York (Denny Chin, Judge), awarded summary judgment to the plaintiffs and enjoined Cablevision from operating the RS-DVR system without licenses from its content providers. At the outset, we think it helpful

to an understanding of our decision to describe, in greater detail, both the RS-DVR and the district court's opinion.

I. Operation of the RS-DVR System

Cable companies like Cablevision aggregate television programming from a wide variety of "content providers"—the various broadcast and cable channels that produce or provide individual programs—and transmit those programs into the homes of their subscribers via coaxial cable. At the outset of the transmission process, Cablevision gathers the content of the various television channels into a single stream of data. Generally, this stream is processed and transmitted to Cablevision's customers in real time. Thus, if a Cartoon Network program is scheduled to air Monday night at 8pm, Cartoon Network transmits that program's data to Cablevision and other cable companies nationwide at that time, and the cable companies immediately re-transmit the data to customers who subscribe to that channel.

Under the new RS-DVR, this single stream of data is split into two streams. The first is routed immediately to customers as before. The second stream flows into a device called the Broadband Media Router ("BMR"), which buffers the data stream, reformats it, and sends it to the "Arroyo Server," which consists, in relevant part, of two data buffers and a number of high-capacity hard disks. The entire stream of data moves to the first buffer (the "primary ingest buffer"), at which point the server automatically inquires as to whether any customers want to record any of that programming. If a customer has requested a particular program, the data for that program move from the primary buffer into a secondary buffer, and then onto a portion of one of the hard disks allocated to that customer. As new data flow into the primary buffer, they overwrite a corresponding quantity of data already on the buffer. The primary ingest buffer holds no more than 0.1 seconds of each channel's programming at any moment. Thus, every tenth of a second, the data residing on this buffer are automatically erased and replaced. The data buffer in the BMR holds no more than 1.2 seconds of programming at any time. While buffering occurs at other points in the operation of the RS-DVR, only the BMR buffer and the primary ingest buffer are utilized absent any request from an individual subscriber.

As the district court observed, "the RS-DVR is not a single piece of equipment," but rather "a complex system requiring numerous computers, processes, networks of cables, and facilities staffed by personnel twenty-four hours a day and seven days a week." To the customer, however, the processes of recording and playback on the RS-DVR are similar to that of a standard set-top DVR. Using a remote control, the customer can record programming by selecting a program in advance from an on-screen guide, or by pressing the record button while viewing a given program. A customer cannot, however, record the earlier portion of a program once it has begun. To begin playback, the customer selects the show from an on-screen list of previously recorded programs. The principal difference in operation is that, instead of sending signals from the remote to an on-set box, the viewer sends signals from the remote, through the cable, to the Arroyo Server at Cablevision's central facility. In this respect, RS-DVR more closely resembles a VOD service, whereby a cable subscriber uses his remote and cable box to request transmission of content, such as a movie, stored on computers at the cable company's facility. But unlike a VOD service, RS-DVR users can only play content that they previously requested to be recorded.

Cablevision has some control over the content available for recording: a customer can only record programs on the channels offered by Cablevision (assuming he subscribes to them). Cablevision can also modify the system to limit the number of channels available and considered doing so during development of the RS-DVR….

DISCUSSION…

"Section 106 of the Copyright Act grants copyright holders a bundle of exclusive rights...." This case implicates two of those rights: the right "to reproduce the copyrighted work in copies," and the right "to perform the copyrighted work publicly." 17 U.S.C. § 106(1), (4). As discussed above, the district court found that Cablevision infringed the first right by 1) buffering the data from its programming stream and 2) copying content onto the Arroyo Server hard disks to enable playback of a program requested by an RS-DVR customer. In addition, the district court found that Cablevision would infringe the public performance right by transmitting a program to an RS-DVR customer in response to that customer's playback request. We address each of these three allegedly infringing acts in turn.

I. The Buffer Data

It is undisputed that Cablevision, not any customer or other entity, takes the content from one stream of programming, after the split, and stores it, one small piece at a time, in the BMR buffer and the primary ingest buffer. As a result, the information is buffered before any customer requests a recording, and would be buffered even if no such request were made. The question is whether, by buffering the data that make up a given work, Cablevision "reproduce[s]" that work "in copies," 17 U.S.C. § 106(1), and thereby infringes the copyright holder's reproduction right.

"Copies," as defined in the Copyright Act, "are material objects ... in which a work is fixed by any method ... and from which the work can be ... reproduced." The Act also provides that a work is "'fixed' in a tangible medium of expression when its embodiment ... is sufficiently permanent or stable to permit it to be ... reproduced ... *for a period of more than transitory duration*." We believe that this language plainly imposes two distinct but related requirements: the work must be embodied in a medium, i.e., placed in a medium such that it can be perceived, reproduced, etc., from that medium (the "embodiment requirement"), and it must remain thus embodied "for a period of more than transitory duration" (the "duration requirement"). Unless both requirements are met, the work is not "fixed" in the buffer, and, as a result, the buffer data is not a "copy" of the original work whose data is buffered.

The district court mistakenly limited its analysis primarily to the embodiment requirement. As a result of this error, once it determined that the buffer data was "[c]learly ... capable of being reproduced," i.e., that the work was embodied in the buffer, the district court concluded that the work was therefore "fixed" in the buffer, and that a copy had thus been made. In doing so, it relied on a line of cases beginning with MAI Systems Corp. v. Peak Computer Inc., 991 F.2d 511 (9th Cir. 1993). It also relied on the United States Copyright Office's 2001 report on the Digital Millennium Copyright Act, which states, in essence, that an embodiment is fixed "[u]nless a reproduction manifests itself so fleetingly that *it cannot be copied*." (emphasis added).

The district court's reliance on cases like *MAI Systems* is misplaced. In general, those cases conclude that an alleged copy is fixed without addressing the duration requirement; it does not follow, however, that those cases assume, much less establish, that such a requirement does not exist. Indeed, the duration requirement, by itself, was not at issue in *MAI Systems* and its progeny. As a result, they do not speak to the issues squarely before us here: If a work is only "embodied" in a medium for a period of transitory duration, can it be "fixed" in that medium, and thus a copy? And what constitutes a period "of more than transitory duration"?

In *MAI Systems*, defendant Peak Computer, Inc., performed maintenance and repairs on computers made and sold by MAI Systems. In order to service a customer's computer, a Peak employee had to operate the computer and run the computer's copyrighted operating system software. The issue in *MAI Systems* was whether, by loading the software into the computer's RAM,[1] the repairman created a "copy" as defined in § 101. The resolution of this issue turned on whether the software's embodiment in the computer's RAM was "fixed," within the meaning of the same section. The Ninth Circuit concluded that

> by showing that Peak loads the software into the RAM and is then able to view the system error log and diagnose the problem with the computer, MAI has adequately shown that the representation created in the RAM is "sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration."

The *MAI Systems* court referenced the "transitory duration" language but did not discuss or analyze it. The opinion notes that the defendants "vigorously" argued that the program's embodiment in the RAM was not a copy, but it does not specify the arguments defendants made. This omission suggests that the parties did not litigate the significance of the "transitory duration" language, and the court therefore had no occasion to address it. This is unsurprising, because it seems fair to assume that in these cases the program was embodied in the RAM for at least several minutes.

Accordingly, we construe *MAI Systems* and its progeny as holding that loading a program into a computer's RAM *can* result in copying that program. We do not read *MAI Systems* as holding that, as a matter of law, loading a program into a form of RAM *always* results in copying. Such a holding would read the "transitory duration" language out of the definition, and we do not believe our sister circuit would dismiss this statutory language without even discussing it. It appears the parties in *MAI Systems* simply did not dispute that the duration requirement was satisfied; this line of cases simply concludes that when a program is loaded into RAM, the embodiment requirement is satisfied—an important holding in itself, and one we see no reason to quibble with here.

At least one court, relying on *MAI Systems* in a highly similar factual setting, has made this point explicitly. In Advanced Computer Services of Michigan, Inc. v. MAI Systems Corp., the district

[1] To run a computer program, the data representing that program must be transferred from a data storage medium (such as a floppy disk or a hard drive) to a form of Random Access Memory ("RAM") where the data can be processed. The data buffers at issue here are also a form of RAM.

court expressly noted that the unlicensed user in that case ran copyrighted diagnostic software "for minutes or longer," but that the program's embodiment in the computer's RAM might be too ephemeral to be fixed if the computer had been shut down "within seconds or fractions of a second" after loading the copyrighted program. We have no quarrel with this reasoning; it merely makes explicit the reasoning that is implicit in the other MAI Systems cases. Accordingly, those cases provide no support for the conclusion that the definition of "fixed" does not include a duration requirement.

Nor does the Copyright Office's 2001 DMCA Report, also relied on by the district court in this case, explicitly suggest that the definition of "fixed" does not contain a duration requirement. However, as noted above, it does suggest that an embodiment is fixed "[u]nless a reproduction manifests itself so fleetingly that it cannot be copied, perceived or communicated." As we have stated, to determine whether a work is "fixed" in a given medium, the statutory language directs us to ask not only 1) whether a work is "embodied" in that medium, but also 2) whether it is embodied in the medium "for a period of more than transitory duration." According to the Copyright Office, if the work is capable of being copied from that medium *for any amount of time*, the answer to both questions is "yes." The problem with this interpretation is that it reads the "transitory duration" language out of the statute.

We assume, as the parties do, that the Copyright Office's pronouncement deserves only *Skidmore* deference, deference based on its "power to persuade." And because the Office's interpretation does not explain why Congress would include language in a definition if it intended courts to ignore that language, we are not persuaded.

In sum, no case law or other authority dissuades us from concluding that the definition of "fixed" imposes both an embodiment requirement and a duration requirement. Accord CoStar Group Inc. v. LoopNet, Inc., 373 F.3d 544, 551 (4th Cir. 2004) (while temporary reproductions "may be made in this transmission process, they would appear not to be 'fixed' in the sense that they are 'of more than transitory duration'"). We now turn to whether, in this case, those requirements are met by the buffer data.

Cablevision does not seriously dispute that copyrighted works are "embodied" in the buffer. Data in the BMR buffer can be reformatted and transmitted to the other components of the RS-DVR system. Data in the primary ingest buffer can be copied onto the Arroyo hard disks if a user has requested a recording of that data. Thus, a work's "embodiment" in either buffer "is sufficiently permanent or stable to permit it to be perceived, reproduced," (as in the case of the ingest buffer) "or otherwise communicated" (as in the BMR buffer). The result might be different if only a single second of a much longer work was placed in the buffer in isolation. In such a situation, it might be reasonable to conclude that only a minuscule portion of a work, rather than "a work" was embodied in the buffer. Here, however, where every second of an entire work is placed, one second at a time, in the buffer, we conclude that the work is embodied in the buffer.

Does any such embodiment last "for a period of more than transitory duration"? No bit of data remains in any buffer for more than a fleeting 1.2 seconds. And unlike the data in cases like *MAI Systems*, which remained embodied in the computer's RAM memory until the user turned the computer off, each bit of data here is rapidly and automatically overwritten as soon as it is

processed. While our inquiry is necessarily fact-specific, and other factors not present here may alter the duration analysis significantly, these facts strongly suggest that the works in this case are embodied in the buffer for only a "transitory" period, thus failing the duration requirement.

Against this evidence, plaintiffs argue only that the duration is not transitory because the data persist "long enough for Cablevision to make reproductions from them." As we have explained above, however, this reasoning impermissibly reads the duration language out of the statute, and we reject it. Given that the data reside in no buffer for more than 1.2 seconds before being automatically overwritten, and in the absence of compelling arguments to the contrary, we believe that the copyrighted works here are not "embodied" in the buffers for a period of more than transitory duration, and are therefore not "fixed" in the buffers. Accordingly, the acts of buffering in the operation of the RS-DVR do not create copies, as the Copyright Act defines that term. Our resolution of this issue renders it unnecessary for us to determine whether any copies produced by buffering data would be de minimis, and we express no opinion on that question.

II. Direct Liability for Creating the Playback Copies

In most copyright disputes, the allegedly infringing act and the identity of the infringer are never in doubt. These cases turn on whether the conduct in question does, in fact, infringe the plaintiff's copyright. In this case, however, the core of the dispute is over the authorship of the infringing conduct. After an RS-DVR subscriber selects a program to record, and that program airs, a copy of the program—a copyrighted work—resides on the hard disks of Cablevision's Arroyo Server, its creation unauthorized by the copyright holder. The question is who made this copy. If it is Cablevision, plaintiffs' theory of direct infringement succeeds; if it is the customer, plaintiffs' theory fails because Cablevision would then face, at most, secondary liability, a theory of liability expressly disavowed by plaintiffs.

Few cases examine the line between direct and contributory liability. Both parties cite a line of cases beginning with Religious Technology Center v. Netcom On-Line Communication Services, 907 F. Supp. 1361 (N.D. Cal. 1995). In *Netcom*, a third-party customer of the defendant Internet service provider ("ISP") posted a copyrighted work that was automatically reproduced by the defendant's computer. The district court refused to impose direct liability on the ISP, reasoning that "[a]lthough copyright is a strict liability statute, there should still be some element of volition or causation which is lacking where a defendant's system is merely used to create a copy by a third party." Recently, the Fourth Circuit endorsed the *Netcom* decision, noting that

> to establish direct liability under ... the Act, something more must be shown than mere ownership of a machine used by others to make illegal copies. There must be actual infringing conduct with a nexus sufficiently close and causal to the illegal copying that one could conclude that the machine owner himself trespassed on the exclusive domain of the copyright owner."

CoStar Group, Inc. v. LoopNet, Inc., 373 F.3d 544, 550 (4th Cir. 2004).

Here, the district court pigeon-holed the conclusions reached in Netcom and its progeny as "premised on the unique attributes of the Internet." While the *Netcom* court was plainly concerned with a theory of direct liability that would effectively "hold the entire Internet liable" for the conduct of a single user, its reasoning and conclusions, consistent with precedents of this court and the Supreme Court, and with the text of the Copyright Act, transcend the Internet. Like the Fourth Circuit, we reject the contention that "the *Netcom* decision was driven by expedience and that its holding is inconsistent with the established law of copyright," and we find it "a particularly rational interpretation of § 106," rather than a special-purpose rule applicable only to ISPs.

When there is a dispute as to the author of an allegedly infringing instance of reproduction, *Netcom* and its progeny direct our attention to the volitional conduct that causes the copy to be made. There are only two instances of volitional conduct in this case: Cablevision's conduct in designing, housing, and maintaining a system that exists only to produce a copy, and a customer's conduct in ordering that system to produce a copy of a specific program. In the case of a VCR, it seems clear—and we know of no case holding otherwise—that the operator of the VCR, the person who actually presses the button to make the recording, supplies the necessary element of volition, not the person who manufactures, maintains, or, if distinct from the operator, owns the machine. We do not believe that an RS-DVR customer is sufficiently distinguishable from a VCR user to impose liability as a direct infringer on a different party for copies that are made automatically upon that customer's command.

The district court emphasized the fact that copying is "instrumental" rather than "incidental" to the function of the RS-DVR system. While that may distinguish the RS-DVR from the ISPs in *Netcom* and *CoStar*, it does not distinguish the RS-DVR from a VCR, a photocopier, or even a typical copy shop. And the parties do not seem to contest that a company that merely makes photocopiers available to the public on its premises, without more, is not subject to liability for direct infringement for reproductions made by customers using those copiers. They only dispute whether Cablevision is similarly situated to such a proprietor.

The district court found Cablevision analogous to a copy shop that makes course packs for college professors. In the leading case involving such a shop, for example, "[t]he professor [gave] the copyshop the materials of which the coursepack [was] to be made up, and the copyshop [did] the rest." Princeton Univ. Press v. Mich. Document Servs., 99 F.3d 1381, 1384 (6th Cir. 1996) (en banc). There did not appear to be any serious dispute in that case that the shop itself was directly liable for reproducing copyrighted works. The district court here found that Cablevision, like this copy shop, would be "doing" the copying, albeit "at the customer's behest."

But because volitional conduct is an important element of direct liability, the district court's analogy is flawed. In determining who actually "makes" a copy, a significant difference exists between making a request to a human employee, who then volitionally operates the copying system to make the copy, and issuing a command directly to a system, which automatically obeys commands and engages in no volitional conduct. In cases like *Princeton University Press*, the defendants operated a copying device and sold the product they made using that device. See 99 F.3d at 1383 ("The corporate defendant ... is a commercial copyshop that reproduced

substantial segments of copyrighted works of scholarship, bound the copies into 'coursepacks,' and sold the coursepacks to students....'). Here, by selling access to a system that automatically produces copies on command, Cablevision more closely resembles a store proprietor who charges customers to use a photocopier on his premises, and it seems incorrect to say, without more, that such a proprietor "makes" any copies when his machines are actually operated by his customers. Some courts have held to the contrary, but they do not explicitly explain why, and we find them unpersuasive. See, e.g., Elektra Records Co. v. Gem Elec. Distribs., Inc., 360 F. Supp. 821, 823 (E.D.N.Y. 1973) (concluding that, "regardless" of whether customers or defendants' employees operated the tape-copying machines at defendants' stores, defendant had actively infringed copyrights).

The district court also emphasized Cablevision's "unfettered discretion in selecting the programming that it would make available for recording." This conduct is indeed more proximate to the creation of illegal copying than, say, operating an ISP or opening a copy shop, where all copied content was supplied by the customers themselves or other third parties. Nonetheless, we do not think it sufficiently proximate to the copying to displace the customer as the person who "makes" the copies when determining liability under the Copyright Act. Cablevision, we note, also has subscribers who use home VCRs or DVRs (like TiVo), and has significant control over the content recorded by these customers. But this control is limited to the channels of programming available to a customer and not to the programs themselves. Cablevision has no control over what programs are made available on individual channels or when those programs will air, if at all. In this respect, Cablevision possesses far less control over recordable content than it does in the VOD context, where it actively selects and makes available beforehand the individual programs available for viewing. For these reasons, we are not inclined to say that Cablevision, rather than the user, "does" the copying produced by the RS-DVR system. As a result, we find that the district court erred in concluding that Cablevision, rather than its RS-DVR customers, makes the copies carried out by the RS-DVR system.

Our refusal to find Cablevision directly liable on these facts is buttressed by the existence and contours of the Supreme Court's doctrine of contributory liability in the copyright context. After all, the purpose of any causation-based liability doctrine is to identify the actor (or actors) whose "conduct has been so significant and important a cause that [he or she] should be legally responsible." But here, to the extent that we may construe the boundaries of direct liability more narrowly, the doctrine of contributory liability stands ready to provide adequate protection to copyrighted works.

Most of the facts found dispositive by the district court—e.g., Cablevision's "continuing relationship" with its RS-DVR customers, its control over recordable content, and the "instrumental[ity]" of copying to the RS-DVR system—seem to us more relevant to the question of contributory liability. In Sony Corp. of America v. Universal City Studios, Inc., the lack of an "ongoing relationship" between Sony and its VCR customers supported the Court's conclusion that it should not impose *contributory* liability on Sony for any infringing copying done by Sony VCR owners. The *Sony* Court did deem it "just" to impose liability on a party in a "position to control" the infringing uses of another, but as a contributory, not direct, infringer. And asking whether copying copyrighted material is only "incidental" to a given technology is akin to asking

whether that technology has "commercially significant noninfringing uses," another inquiry the Sony Court found relevant to whether imposing *contributory* liability was just.

The Supreme Court's desire to maintain a meaningful distinction between direct and contributory copyright infringement is consistent with congressional intent. The Patent Act, unlike the Copyright Act, expressly provides that someone who "actively induces infringement of a patent" is "liable as an infringer," just like someone who commits the underlying infringing act by "us[ing]" a patented invention without authorization. In contrast, someone who merely "sells ... a material or apparatus for use in practicing a patented process" faces only liability as a "contributory infringer." If Congress had meant to assign direct liability to both the person who actually commits a copyright-infringing act and any person who actively induces that infringement, the Patent Act tells us that it knew how to draft a statute that would have this effect. Because Congress did not do so, the *Sony* Court concluded that "[t]he Copyright Act does not expressly render anyone liable for infringement committed by another." Furthermore, in cases like *Sony*, the Supreme Court has strongly signaled its intent to use the doctrine of contributory infringement, not direct infringement, to "identify[ ] the circumstances in which it is just to hold one individual accountable for the actions of another." Thus, although *Sony* warns us that "the lines between direct infringement, contributory infringement, and vicarious liability are not clearly drawn," that decision does not absolve us of our duty to discern where that line falls in cases, like this one, that require us to decide the question.

The district court apparently concluded that Cablevision's operation of the RS-DVR system would contribute in such a major way to the copying done by another that it made sense to say that Cablevision was a direct infringer, and thus, in effect, was "doing" the relevant copying. There are certainly other cases, not binding on us, that follow this approach. See, e.g., Playboy Enters. v. Russ Hardenburgh, Inc., 982 F. Supp. 503, 513 (N.D. Ohio 1997) (noting that defendant ISP's encouragement of its users to copy protected files was "crucial" to finding that it was a direct infringer). We need not decide today whether one's contribution to the creation of an infringing copy may be so great that it warrants holding that party directly liable for the infringement, even though another party has actually made the copy. We conclude only that on the facts of this case, copies produced by the RS-DVR system are "made" by the RS-DVR customer, and Cablevision's contribution to this reproduction by providing the system does not warrant the imposition of direct liability. Therefore, Cablevision is entitled to summary judgment on this point, and the district court erred in awarding summary judgment to plaintiffs….

[In the third section, the Second Circuit held that Cablevision's playback of the recording did not constitute an infringing public performance:

> Because each RS-DVR playback transmission is made to a single subscriber using a single unique copy produced by that subscriber, we conclude that such transmissions are not performances "to the public," and therefore do not infringe any exclusive right of public performance.]

17 U.S.C. § 506(a). Criminal Infringement.

(1) In general. — Any person who willfully infringes a copyright shall be punished as provided under section 2319 of title 18, if the infringement was committed —

> (A) for purposes of commercial advantage or private financial gain;
>
> (B) by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000; or
>
> (C) by the distribution of a work being prepared for commercial distribution, by making it available on a computer network accessible to members of the public, if such person knew or should have known that the work was intended for commercial distribution.

(2) Evidence. — For purposes of this subsection, evidence of reproduction or distribution of a copyrighted work, by itself, shall not be sufficient to establish willful infringement of a copyright.

(3) Definition. — In this subsection, the term "work being prepared for commercial distribution" means —

> (A) a computer program, a musical work, a motion picture or other audiovisual work, or a sound recording, if, at the time of unauthorized distribution —
>
> (i) the copyright owner has a reasonable expectation of commercial distribution; and
> (ii) the copies or phonorecords of the work have not been commercially distributed; or
>
> (B) a motion picture, if, at the time of unauthorized distribution, the motion picture —
>
> (i) has been made available for viewing in a motion picture exhibition facility; and
> (ii) has not been made available in copies for sale to the general public in the United States in a format intended to permit viewing outside a motion picture exhibition facility.

BMG Music v. Gonzalez, 430 F.3d 888 (7th Cir. 2005).
Easterbrook, Circuit Judge.

Last June the Supreme Court held in MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005), that a distributed file-sharing system is engaged in contributory copyright infringement when its principal object is the dissemination of copyrighted material. The foundation of this holding is a belief that people who post or download music files are primary infringers. In re Aimster Copyright Litigation, 334 F.3d 643, 645 (7th Cir. 2003), which anticipated *Grokster*, made the same assumption. In this appeal Cecilia Gonzalez, who downloaded copyrighted music through the KaZaA file-sharing network, denies the premise of *Grokster* and *Aimster*. She contends that her activities were fair use rather than infringement. The district court disagreed and granted summary judgment for the copyright proprietors (to which we refer collectively as BMG Music). The court enjoined Gonzalez from further infringement and awarded $22,500 in damages under 17 U.S.C. § 504(c).

A "fair use" of copyrighted material is not infringement. Gonzalez insists that she was engaged in fair use under the terms of 17 U.S.C. § 107—or at least that a material dispute entitles her to a trial. It is undisputed, however, that she downloaded more than 1,370 copyrighted songs during a few weeks and kept them on her computer until she was caught. Her position is that she was just sampling music to determine what she liked enough to buy at retail. Because this suit was resolved on summary judgment, we must assume that Gonzalez is telling the truth when she says that she owned compact discs containing some of the songs before she downloaded them and that she purchased others later. She concedes, however, that she has never owned legitimate copies of 30 songs that she downloaded. (How many of the remainder she owned is disputed.)

Instead of erasing songs that she decided not to buy, she retained them. It is these 30 songs about which there is no dispute concerning ownership that formed the basis of the damages award. This is not a form of time-shifting, along the lines of Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984) ("Betamax"). A copy downloaded, played, and retained on one's hard drive for future use is a direct substitute for a purchased copy—and without the benefit of the license fee paid to the broadcaster. The premise of *Betamax* is that the broadcast was licensed for one transmission and thus one viewing. *Betamax* held that shifting the time of this single viewing is fair use. The files that Gonzalez obtained, by contrast, were posted in violation of copyright law; there was no license covering a single transmission or hearing—and, to repeat, Gonzalez kept the copies. Time-shifting by an authorized recipient this is not.

Section 107 provides that when considering a defense of fair use the court must take into account "(1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work." Gonzalez was not engaged in a nonprofit use; she downloaded (and kept) whole copyrighted songs (for which, as with poetry, copying of more than a couplet or two is deemed excessive); and she did this despite the fact that these works often are sold per song as well as per album. This leads her to concentrate on the fourth consideration: "the effect of the use upon the potential market for or value of the copyrighted work."

As she tells the tale, downloading on a try-before-you-buy basis is good advertising for copyright proprietors, expanding the value of their inventory. The Supreme Court thought otherwise in *Grokster*, with considerable empirical support. As file sharing has increased over the last four years, the sales of recorded music have dropped by approximately 30%. Perhaps other economic factors contributed, but the events likely are related. Music downloaded for free from the Internet is a close substitute for purchased music; many people are bound to keep the downloaded files without buying originals. That is exactly what Gonzalez did for at least 30 songs. It is no surprise, therefore, that the only appellate decision on point has held that downloading copyrighted songs cannot be defended as fair use, whether or not the recipient plans to buy songs she likes well enough to spring for. See A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1014-19 (9th Cir. 2001). See also UMG Recordings, Inc. v. MP3.com, Inc., 92 F. Supp. 2d 349 (S.D.N.Y. 2000) (holding that downloads are not fair use even if the downloader already owns one purchased copy).

Although BMG Music sought damages for only the 30 songs that Gonzalez concedes she has never purchased, all 1,000+ of her downloads violated the statute. All created copies of an entire work. All undermined the means by which authors seek to profit. Gonzalez proceeds as if the authors' only interest were in selling compact discs containing collections of works. Not so; there is also a market in ways to introduce potential consumers to music.

Think of radio. Authors and publishers collect royalties on the broadcast of recorded music, even though these broadcasts may boost sales. Downloads from peer-to-peer networks such as KaZaA compete with licensed broadcasts and hence undermine the income available to authors. This is true even if a particular person never buys recorded media. Many radio stations stream their content over the Internet, paying a fee for the right to do so. Gonzalez could have listened to this streaming music to sample songs for purchase; had she done so, the authors would have received royalties from the broadcasters (and reduced the risk that files saved to disk would diminish the urge to pay for the music in the end).

Licensed Internet sellers, such as the iTunes Music Store, offer samples—but again they pay authors a fee for the right to do so, and the teasers are just a portion of the original. Other intermediaries (not only Yahoo! Music Unlimited and Real Rhapsody but also the revived Napster, with a new business model) offer licensed access to large collections of music; customers may rent the whole library by the month or year, sample them all, and purchase any songs they want to keep. New technologies, such as SNOCAP, enable authorized trials over peer-to-peer systems.

Authorized previews share the feature of evanescence: if a listener decides not to buy (or stops paying the rental fee), no copy remains behind. With all of these means available to consumers who want to choose where to spend their money, downloading full copies of copyrighted material without compensation to authors cannot be deemed "fair use." Copyright law lets authors make their own decisions about how best to promote their works; copiers such as Gonzalez cannot ask courts (and juries) to second-guess the market and call wholesale copying "fair use" if they think that authors err in understanding their own economic interests or that Congress erred in granting authors the rights in the copyright statute. Nor can she defend by

observing that other persons were greater offenders; Gonzalez's theme that she obtained "only 30" (or "only 1,300") copyrighted songs is no more relevant than a thief's contention that he shoplifted "only 30" compact discs, planning to listen to them at home and pay later for any he liked.

BMG Music elected to seek statutory damages under 17 U.S.C. § 504(c)(1) instead of proving actual injury. This section provides that the author's entitlement, per infringed work, is "a sum of not less than $750 or more than $30,000 as the court considers just." But if an "infringer sustains the burden of proving, and the court finds, that such infringer was not aware and had no reason to believe that his or her acts constituted an infringement of copyright, the court in its discretion may reduce the award of statutory damages to a sum of not less than $200." 17 U.S.C. § 504(c)(2). Gonzalez asked the district court to reduce the award under this proviso, but the judge concluded that § 402(d) bars any reduction in the minimum award. This subsection provides: "If a notice of copyright in the form and position specified by this section appears on the published phonorecord or phonorecords to which a defendant in a copyright infringement suit had access, then no weight shall be given to such a defendant's interposition of a defense based on innocent infringement in mitigation of actual or statutory damages". It is undisputed that BMG Music gave copyright notice as required—"on the surface of the phonorecord, or on the phonorecord label or container" (§ 402(c)). It is likewise undisputed that Gonzalez had "access" to records and compact disks bearing the proper notice. She downloaded data rather than discs, and the data lacked copyright notices, but the statutory question is whether "access" to legitimate works was available rather than whether infringers earlier in the chain attached copyright notices to the pirated works. Gonzalez readily could have learned, had she inquired, that the music was under copyright.

If BMG Music had requested more than $750 per work, then Gonzalez would have been entitled to a trial. See Feltner v. Columbia Pictures Television, Inc., 523 U.S. 340 (1998). What number between $750 and $30,000 is "just" recompense is a question for the jury, unless both sides agree to decision by the court. But BMG Music was content with $750 per song, which the district judge awarded on summary judgment. Gonzalez contends that this was improper: *Feltner*, she contends, holds that a jury must decide whether even the statutory minimum award will be allowed.

Feltner holds that a claim for statutory damages under § 504(c) is a suit at law to which the seventh amendment applies. This does not mean, however, that a jury must resolve every dispute. When there are no disputes of material fact, the court may enter summary judgment without transgressing the Constitution. While acknowledging this proposition, Gonzalez insists that copyright cases are different. She relies entirely on a single passage from *Feltner*: "The right to a jury trial includes the right to have a jury determine the *amount* of statutory damages, if any, awarded to the copyright owner." (emphasis in original). Gonzalez maintains that by adding "if any" the Court allowed a jury to send an author home empty handed, even if the statute makes $750 the minimum. In other words, she contends that *Feltner* creates a system of jury nullification unique to copyright litigation.

The Justices did not purport to give defendants in copyright cases the right to ask jurors to return verdicts in the teeth of the law. The sentence we have quoted is a general description of the

jury's role, which the Court drew from seventeenth-century English jurisprudence. That's hardly a plausible source for a rule unique to American copyright law. In *Feltner* neither side had sought summary judgment. We read *Feltner* as establishing no more (and no less) than that cases under § 504(c) are normal civil actions subject to the normal allocation of functions between judge and jury. When there is a material dispute of fact to be resolved or discretion to be exercised in selecting a financial award, then either side is entitled to a jury; if there is no material dispute and a rule of law eliminates discretion in selecting the remedy, then summary judgment is permissible.

Gonzalez says that the ninth circuit understood *Feltner* differently on remand, but that's mistaken. A jury trial was held—for there were material factual disputes—and the jury returned a verdict of $31.68 million in statutory damages (or $72,000 per infringed work, an award made possible by the jury's conclusion that infringement had been wilful). The defendant, ruing its Pyrrhic victory in the Supreme Court (the judge's original award, which the Court vacated, had been $8.8 million), maintained that § 504(c) is unconstitutional, and that only actual damages may be awarded, because § 504(c) does not provide for a jury trial. The court of appeals rejected that contention, noting that after the Supreme Court's decision a jury trial had been held. Whether a jury resolves the dispute because of statutory language or because of the seventh amendment is all the same to the litigants. It is not possible to find, in a decision affirming a jury's verdict, a rule of law that a jury is required even when there are no factual disputes to resolve and no discretion to exercise.

As for the injunction: Gonzalez contends that this should be vacated because she has learned her lesson, has dropped her broadband access to the Internet, and is unlikely to download copyrighted material again. A private party's discontinuation of unlawful conduct does not make the dispute moot, however. An injunction remains appropriate to ensure that the misconduct does not recur as soon as the case ends. The district court did not abuse its discretion in awarding prospective relief.

Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).
Souter, Justice.

The question is under what circumstances the distributor of a product capable of both lawful and unlawful use is liable for acts of copyright infringement by third parties using the product. We hold that one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties.

I
A

Respondents, Grokster, Ltd., and StreamCast Networks, Inc., defendants in the trial court, distribute free software products that allow computer users to share electronic files through peer-to-peer networks, so called because users' computers communicate directly with each other, not through central servers. The advantage of peer-to-peer networks over information networks of other types shows up in their substantial and growing popularity. Because they need no central computer server to mediate the exchange of information or files among users, the high-bandwidth communications capacity for a server may be dispensed with, and the need for costly server storage space is eliminated. Since copies of a file (particularly a popular one) are available on many users' computers, file requests and retrievals may be faster than on other types of networks, and since file exchanges do not travel through a server, communications can take place between any computers that remain connected to the network without risk that a glitch in the server will disable the network in its entirety. Given these benefits in security, cost, and efficiency, peer-to-peer networks are employed to store and distribute electronic files by universities, government agencies, corporations, and libraries, among others.[1]

Other users of peer-to-peer networks include individual recipients of Grokster's and StreamCast's software, and although the networks that they enjoy through using the software can be used to share any type of digital file, they have prominently employed those networks in sharing copyrighted music and video files without authorization. A group of copyright holders (MGM for short, but including motion picture studios, recording companies, songwriters, and music publishers) sued Grokster and StreamCast for their users' copyright infringements, alleging that they knowingly and intentionally distributed their software to enable users to reproduce and distribute the copyrighted works in violation of the Copyright Act, 17 U.S.C. § 101 et seq. MGM sought damages and an injunction.

Discovery during the litigation revealed the way the software worked, the business aims of each defendant company, and the predilections of the users. Grokster's eponymous software employs what is known as FastTrack technology, a protocol developed by others and licensed to Grokster. StreamCast distributes a very similar product except that its software, called Morpheus, relies on

[1] Peer-to-peer networks have disadvantages as well. Searches on peer-to-peer networks may not reach and uncover all available files because search requests may not be transmitted to every computer on the network. There may be redundant copies of popular files. The creator of the software has no incentive to minimize storage or bandwidth consumption, the costs of which are borne by every user of the network. Most relevant here, it is more difficult to control the content of files available for retrieval and the behavior of users.

what is known as Gnutella technology. A user who downloads and installs either software possesses the protocol to send requests for files directly to the computers of others using software compatible with FastTrack or Gnutella. On the FastTrack network opened by the Grokster software, the user's request goes to a computer given an indexing capacity by the software and designated a supernode, or to some other computer with comparable power and capacity to collect temporary indexes of the files available on the computers of users connected to it. The supernode (or indexing computer) searches its own index and may communicate the search request to other supernodes. If the file is found, the supernode discloses its location to the computer requesting it, and the requesting user can download the file directly from the computer located. The copied file is placed in a designated sharing folder on the requesting user's computer, where it is available for other users to download in turn, along with any other file in that folder.

In the Gnutella network made available by Morpheus, the process is mostly the same, except that in some versions of the Gnutella protocol there are no supernodes. In these versions, peer computers using the protocol communicate directly with each other. When a user enters a search request into the Morpheus software, it sends the request to computers connected with it, which in turn pass the request along to other connected peers. The search results are communicated to the requesting computer, and the user can download desired files directly from peers' computers. As this description indicates, Grokster and StreamCast use no servers to intercept the content of the search requests or to mediate the file transfers conducted by users of the software, there being no central point through which the substance of the communications passes in either direction.[4]

Although Grokster and StreamCast do not therefore know when particular files are copied, a few searches using their software would show what is available on the networks the software reaches. MGM commissioned a statistician to conduct a systematic search, and his study showed that nearly 90% of the files available for download on the FastTrack system were copyrighted works.[5] Grokster and StreamCast dispute this figure, raising methodological problems and arguing that free copying even of copyrighted works may be authorized by the rightholders. They also argue that potential noninfringing uses of their software are significant in kind, even if infrequent in practice. Some musical performers, for example, have gained new audiences by distributing their copyrighted works for free across peer-to-peer networks, and some distributors of unprotected content have used peer-to-peer networks to disseminate files, Shakespeare being an example. Indeed, StreamCast has given Morpheus users the opportunity to download the briefs in this very case, though their popularity has not been quantified.

As for quantification, the parties' anecdotal and statistical evidence entered thus far to show the content available on the FastTrack and Gnutella networks does not say much about which files are actually downloaded by users, and no one can say how often the software is used to obtain copies of unprotected material. But MGM's evidence gives reason to think that the vast majority of users' downloads are acts of infringement, and because well over 100 million copies of the

[4] There is some evidence that both Grokster and StreamCast previously operated supernodes, which compiled indexes of files available on all of the nodes connected to them. This evidence, pertaining to previous versions of the defendants' software, is not before us and would not affect our conclusions in any event.

[5] By comparison, evidence introduced by the plaintiffs in A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (C.A.9 2001), showed that 87% of files available on the Napster file-sharing network were copyrighted.

software in question are known to have been downloaded, and billions of files are shared across the FastTrack and Gnutella networks each month, the probable scope of copyright infringement is staggering.

Grokster and StreamCast concede the infringement in most downloads, and it is uncontested that they are aware that users employ their software primarily to download copyrighted files, even if the decentralized FastTrack and Gnutella networks fail to reveal which files are being copied, and when. From time to time, moreover, the companies have learned about their users' infringement directly, as from users who have sent e-mail to each company with questions about playing copyrighted movies they had downloaded, to whom the companies have responded with guidance. And MGM notified the companies of 8 million copyrighted files that could be obtained using their software.

Grokster and StreamCast are not, however, merely passive recipients of information about infringing use. The record is replete with evidence that from the moment Grokster and StreamCast began to distribute their free software, each one clearly voiced the objective that recipients use it to download copyrighted works, and each took active steps to encourage infringement.

After the notorious file-sharing service, Napster, was sued by copyright holders for facilitation of copyright infringement, A&M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896 (N.D. Cal. 2000), aff'd in part, rev'd in part, 239 F.3d 1004 (C.A.9 2001), StreamCast gave away a software program of a kind known as OpenNap, designed as compatible with the Napster program and open to Napster users for downloading files from other Napster and OpenNap users' computers. Evidence indicates that "[i]t was always [StreamCast's] intent to use [its OpenNap network] to be able to capture email addresses of [its] initial target market so that [it] could promote [its] StreamCast Morpheus interface to them"; indeed, the OpenNap program was engineered "'to leverage Napster's 50 million user base.'"

StreamCast monitored both the number of users downloading its OpenNap program and the number of music files they downloaded. It also used the resulting OpenNap network to distribute copies of the Morpheus software and to encourage users to adopt it. Internal company documents indicate that StreamCast hoped to attract large numbers of former Napster users if that company was shut down by court order or otherwise, and that StreamCast planned to be the next Napster. A kit developed by StreamCast to be delivered to advertisers, for example, contained press articles about StreamCast's potential to capture former Napster users, and it introduced itself to some potential advertisers as a company "which is similar to what Napster was." It broadcast banner advertisements to users of other Napster-compatible software, urging them to adopt its OpenNap. An internal e-mail from a company executive stated: "'We have put this network in place so that when Napster pulls the plug on their free service ... or if the Court orders them shut down prior to that ... we will be positioned to capture the flood of their 32 million users that will be actively looking for an alternative.'"

Thus, StreamCast developed promotional materials to market its service as the best Napster alternative. One proposed advertisement read: "Napster Inc. has announced that it will soon begin charging you a fee. That's if the courts don't order it shut down first. What will you do to

get around it?" Another proposed ad touted StreamCast's software as the "# 1 alternative to Napster" and asked "[w]hen the lights went off at Napster ... where did the users go?" (ellipsis in original).[7] StreamCast even planned to flaunt the illegal uses of its software; when it launched the OpenNap network, the chief technology officer of the company averred that "[t]he goal is to get in trouble with the law and get sued. It's the best way to get in the new[s]."

The evidence that Grokster sought to capture the market of former Napster users is sparser but revealing, for Grokster launched its own OpenNap system called Swaptor and inserted digital codes into its Web site so that computer users using Web search engines to look for "Napster" or "[f]ree file sharing" would be directed to the Grokster Web site, where they could download the Grokster software. And Grokster's name is an apparent derivative of Napster.

StreamCast's executives monitored the number of songs by certain commercial artists available on their networks, and an internal communication indicates they aimed to have a larger number of copyrighted songs available on their networks than other file-sharing networks. The point, of course, would be to attract users of a mind to infringe, just as it would be with their promotional materials developed showing copyrighted songs as examples of the kinds of files available through Morpheus. Morpheus in fact allowed users to search specifically for "Top 40" songs, which were inevitably copyrighted. Similarly, Grokster sent users a newsletter promoting its ability to provide particular, popular copyrighted materials.

In addition to this evidence of express promotion, marketing, and intent to promote further, the business models employed by Grokster and StreamCast confirm that their principal object was use of their software to download copyrighted works. Grokster and StreamCast receive no revenue from users, who obtain the software itself for nothing. Instead, both companies generate income by selling advertising space, and they stream the advertising to Grokster and Morpheus users while they are employing the programs. As the number of users of each program increases, advertising opportunities become worth more. While there is doubtless some demand for free Shakespeare, the evidence shows that substantive volume is a function of free access to copyrighted work. Users seeking Top 40 songs, for example, or the latest release by Modest Mouse, are certain to be far more numerous than those seeking a free Decameron, and Grokster and StreamCast translated that demand into dollars.

Finally, there is no evidence that either company made an effort to filter copyrighted material from users' downloads or otherwise impede the sharing of copyrighted files. Although Grokster appears to have sent e-mails warning users about infringing content when it received threatening notice from the copyright holders, it never blocked anyone from continuing to use its software to share copyrighted files. StreamCast not only rejected another company's offer of help to monitor infringement, but blocked the Internet Protocol addresses of entities it believed were trying to engage in such monitoring on its networks….

II

A

[7] The record makes clear that StreamCast developed these promotional materials but not whether it released them to the public. Even if these advertisements were not released to the public and do not show encouragement to infringe, they illuminate StreamCast's purposes.

MGM and many of the *amici* fault the Court of Appeals's holding for upsetting a sound balance between the respective values of supporting creative pursuits through copyright protection and promoting innovation in new communication technologies by limiting the incidence of liability for copyright infringement. The more artistic protection is favored, the more technological innovation may be discouraged; the administration of copyright law is an exercise in managing the tradeoff. See Sony Corp. v. Universal City Studios, supra, at 442.

The tension between the two values is the subject of this case, with its claim that digital distribution of copyrighted material threatens copyright holders as never before, because every copy is identical to the original, copying is easy, and many people (especially the young) use file-sharing software to download copyrighted works. This very breadth of the software's use may well draw the public directly into the debate over copyright policy, and the indications are that the ease of copying songs or movies using software like Grokster's and Napster's is fostering disdain for copyright protection. As the case has been presented to us, these fears are said to be offset by the different concern that imposing liability, not only on infringers but on distributors of software based on its potential for unlawful use, could limit further development of beneficial technologies.[8]

The argument for imposing indirect liability in this case is, however, a powerful one, given the number of infringing downloads that occur every day using StreamCast's and Grokster's software. When a widely shared service or product is used to commit infringement, it may be impossible to enforce rights in the protected work effectively against all direct infringers, the only practical alternative being to go against the distributor of the copying device for secondary liability on a theory of contributory or vicarious infringement.

One infringes contributorily by intentionally inducing or encouraging direct infringement, see Gershwin Pub. Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1162 (C.A.2 1971), and infringes vicariously by profiting from direct infringement while declining to exercise a right to stop or limit it, Shapiro, Bernstein & Co. v. H.L. Green Co., 316 F.2d 304, 307 (C.A.2 1963).[9] Although "[t]he Copyright Act does not expressly render anyone liable for infringement committed by another," Sony Corp. v. Universal City Studios, 464 U.S., at 434, these doctrines of secondary liability emerged from common law principles and are well established in the law.

B

[8] The mutual exclusivity of these values should not be overstated, however. On the one hand technological innovators, including those writing file-sharing computer programs, may wish for effective copyright protections for their work. On the other hand the widespread distribution of creative works through improved technologies may enable the synthesis of new works or generate audiences for emerging artists.

[9] We stated in Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984), that "'the lines between direct infringement, contributory infringement and vicarious liability are not clearly drawn' ....[R]easoned analysis of [the Sony plaintiffs' contributory infringement claim] necessarily entails consideration of arguments and case law which may also be forwarded under the other labels, and indeed the parties ... rely upon such arguments and authority in support of their respective positions on the issue of contributory infringement." In the present case MGM has argued a vicarious liability theory, which allows imposition of liability when the defendant profits directly from the infringement and has a right and ability to supervise the direct infringer, even if the defendant initially lacks knowledge of the infringement. Because we resolve the case based on an inducement theory, there is no need to analyze separately MGM's vicarious liability theory.

Despite the currency of these principles of secondary liability, this Court has dealt with secondary copyright infringement in only one recent case, and because MGM has tailored its principal claim to our opinion there, a look at our earlier holding is in order. In Sony Corp. v. Universal City Studios, this Court addressed a claim that secondary liability for infringement can arise from the very distribution of a commercial product. There, the product, novel at the time, was what we know today as the videocassette recorder or VCR. Copyright holders sued Sony as the manufacturer, claiming it was contributorily liable for infringement that occurred when VCR owners taped copyrighted programs because it supplied the means used to infringe, and it had constructive knowledge that infringement would occur. At the trial on the merits, the evidence showed that the principal use of the VCR was for "'time-shifting,'" or taping a program for later viewing at a more convenient time, which the Court found to be a fair, not an infringing, use. There was no evidence that Sony had expressed an object of bringing about taping in violation of copyright or had taken active steps to increase its profits from unlawful taping. Although Sony's advertisements urged consumers to buy the VCR to "'record favorite shows'" or "'build a library'" of recorded programs, neither of these uses was necessarily infringing.

On those facts, with no evidence of stated or indicated intent to promote infringing uses, the only conceivable basis for imposing liability was on a theory of contributory infringement arising from its sale of VCRs to consumers with knowledge that some would use them to infringe. But because the VCR was "capable of commercially significant noninfringing uses," we held the manufacturer could not be faulted solely on the basis of its distribution.

This analysis reflected patent law's traditional staple article of commerce doctrine, now codified, that distribution of a component of a patented device will not violate the patent if it is suitable for use in other ways. 35 U.S.C. § 271(c). The doctrine was devised to identify instances in which it may be presumed from distribution of an article in commerce that the distributor intended the article to be used to infringe another's patent, and so may justly be held liable for that infringement. "One who makes and sells articles which are only adapted to be used in a patented combination will be presumed to intend the natural consequences of his acts; he will be presumed to intend that they shall be used in the combination of the patent."

In sum, where an article is "good for nothing else" but infringement, there is no legitimate public interest in its unlicensed availability, and there is no injustice in presuming or imputing an intent to infringe. Conversely, the doctrine absolves the equivocal conduct of selling an item with substantial lawful as well as unlawful uses, and limits liability to instances of more acute fault than the mere understanding that some of one's products will be misused. It leaves breathing room for innovation and a vigorous commerce.

The parties and many of the *amici* in this case think the key to resolving it is the *Sony* rule and, in particular, what it means for a product to be "capable of commercially significant noninfringing uses." Sony Corp. v. Universal City Studios, supra, at 442. MGM advances the argument that granting summary judgment to Grokster and StreamCast as to their current activities gave too much weight to the value of innovative technology, and too little to the copyrights infringed by users of their software, given that 90% of works available on one of the networks was shown to be copyrighted. Assuming the remaining 10% to be its noninfringing use, MGM says this should

not qualify as "substantial," and the Court should quantify *Sony* to the extent of holding that a product used "principally" for infringement does not qualify. As mentioned before, Grokster and StreamCast reply by citing evidence that their software can be used to reproduce public domain works, and they point to copyright holders who actually encourage copying. Even if infringement is the principal practice with their software today, they argue, the noninfringing uses are significant and will grow.

We agree with MGM that the Court of Appeals misapplied *Sony*, which it read as limiting secondary liability quite beyond the circumstances to which the case applied. *Sony* barred secondary liability based on presuming or imputing intent to cause infringement solely from the design or distribution of a product capable of substantial lawful use, which the distributor knows is in fact used for infringement. The Ninth Circuit has read *Sony's* limitation to mean that whenever a product is capable of substantial lawful use, the producer can never be held contributorily liable for third parties' infringing use of it; it read the rule as being this broad, even when an actual purpose to cause infringing use is shown by evidence independent of design and distribution of the product, unless the distributors had "specific knowledge of infringement at a time at which they contributed to the infringement, and failed to act upon that information." Because the Circuit found the StreamCast and Grokster software capable of substantial lawful use, it concluded on the basis of its reading of *Sony* that neither company could be held liable, since there was no showing that their software, being without any central server, afforded them knowledge of specific unlawful uses.

This view of *Sony*, however, was error, converting the case from one about liability resting on imputed intent to one about liability on any theory. Because *Sony* did not displace other theories of secondary liability, and because we find below that it was error to grant summary judgment to the companies on MGM's inducement claim, we do not revisit *Sony* further, as MGM requests, to add a more quantified description of the point of balance between protection and commerce when liability rests solely on distribution with knowledge that unlawful use will occur. It is enough to note that the Ninth Circuit's judgment rested on an erroneous understanding of *Sony* and to leave further consideration of the *Sony* rule for a day when that may be required.

C

Sony's rule limits imputing culpable intent as a matter of law from the characteristics or uses of a distributed product. But nothing in *Sony* requires courts to ignore evidence of intent if there is such evidence, and the case was never meant to foreclose rules of fault-based liability derived from the common law.[10] Sony Corp. v. Universal City Studios, supra, at 439 ("If vicarious liability is to be imposed on Sony in this case, it must rest on the fact that it has sold equipment with constructive knowledge" of the potential for infringement). Thus, where evidence goes beyond a product's characteristics or the knowledge that it may be put to infringing uses, and shows statements or actions directed to promoting infringement, *Sony's* staple-article rule will not preclude liability.

[10] Nor does the Patent Act's exemption from liability for those who distribute a staple article of commerce, 35 U.S.C. § 271(c), extend to those who induce patent infringement, § 271(b).

The classic case of direct evidence of unlawful purpose occurs when one induces commission of infringement by another, or "entic[es] or persuad[es] another" to infringe, as by advertising. Thus at common law a copyright or patent defendant who "not only expected but invoked [infringing use] by advertisement" was liable for infringement "on principles recognized in every part of the law."

The rule on inducement of infringement as developed in the early cases is no different today. Evidence of "active steps ... taken to encourage direct infringement," such as advertising an infringing use or instructing how to engage in an infringing use, show an affirmative intent that the product be used to infringe, and a showing that infringement was encouraged overcomes the law's reluctance to find liability when a defendant merely sells a commercial product suitable for some lawful use.

For the same reasons that *Sony* took the staple-article doctrine of patent law as a model for its copyright safe-harbor rule, the inducement rule, too, is a sensible one for copyright. We adopt it here, holding that one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties. We are, of course, mindful of the need to keep from trenching on regular commerce or discouraging the development of technologies with lawful and unlawful potential. Accordingly, just as *Sony* did not find intentional inducement despite the knowledge of the VCR manufacturer that its device could be used to infringe, mere knowledge of infringing potential or of actual infringing uses would not be enough here to subject a distributor to liability. Nor would ordinary acts incident to product distribution, such as offering customers technical support or product updates, support liability in themselves. The inducement rule, instead, premises liability on purposeful, culpable expression and conduct, and thus does nothing to compromise legitimate commerce or discourage innovation having a lawful promise.

III

A

The only apparent question about treating MGM's evidence as sufficient to withstand summary judgment under the theory of inducement goes to the need on MGM's part to adduce evidence that StreamCast and Grokster communicated an inducing message to their software users. The classic instance of inducement is by advertisement or solicitation that broadcasts a message designed to stimulate others to commit violations. MGM claims that such a message is shown here. It is undisputed that StreamCast beamed onto the computer screens of users of Napster-compatible programs ads urging the adoption of its OpenNap program, which was designed, as its name implied, to invite the custom of patrons of Napster, then under attack in the courts for facilitating massive infringement. Those who accepted StreamCast's OpenNap program were offered software to perform the same services, which a factfinder could conclude would readily have been understood in the Napster market as the ability to download copyrighted music files. Grokster distributed an electronic newsletter containing links to articles promoting its software's ability to access popular copyrighted music. And anyone whose Napster or free file-sharing searches turned up a link to Grokster would have understood Grokster to be offering the same file-sharing ability as Napster, and to the same people who probably used Napster for infringing

downloads; that would also have been the understanding of anyone offered Grokster's suggestively named Swaptor software, its version of OpenNap. And both companies communicated a clear message by responding affirmatively to requests for help in locating and playing copyrighted materials.

In StreamCast's case, of course, the evidence just described was supplemented by other unequivocal indications of unlawful purpose in the internal communications and advertising designs aimed at Napster users ("When the lights went off at Napster ... where did the users go?"). Whether the messages were communicated is not to the point on this record. The function of the message in the theory of inducement is to prove by a defendant's own statements that his unlawful purpose disqualifies him from claiming protection (and incidentally to point to actual violators likely to be found among those who hear or read the message). Proving that a message was sent out, then, is the preeminent but not exclusive way of showing that active steps were taken with the purpose of bringing about infringing acts, and of showing that infringing acts took place by using the device distributed. Here, the summary judgment record is replete with other evidence that Grokster and StreamCast, unlike the manufacturer and distributor in *Sony*, acted with a purpose to cause copyright violations by use of software suitable for illegal use.

Three features of this evidence of intent are particularly notable. First, each company showed itself to be aiming to satisfy a known source of demand for copyright infringement, the market comprising former Napster users. StreamCast's internal documents made constant reference to Napster, it initially distributed its Morpheus software through an OpenNap program compatible with Napster, it advertised its OpenNap program to Napster users, and its Morpheus software functions as Napster did except that it could be used to distribute more kinds of files, including copyrighted movies and software programs. Grokster's name is apparently derived from Napster, it too initially offered an OpenNap program, its software's function is likewise comparable to Napster's, and it attempted to divert queries for Napster onto its own Web site. Grokster and StreamCast's efforts to supply services to former Napster users, deprived of a mechanism to copy and distribute what were overwhelmingly infringing files, indicate a principal, if not exclusive, intent on the part of each to bring about infringement.

Second, this evidence of unlawful objective is given added significance by MGM's showing that neither company attempted to develop filtering tools or other mechanisms to diminish the infringing activity using their software. While the Ninth Circuit treated the defendants' failure to develop such tools as irrelevant because they lacked an independent duty to monitor their users' activity, we think this evidence underscores Grokster's and StreamCast's intentional facilitation of their users' infringement.[12]

Third, there is a further complement to the direct evidence of unlawful objective. It is useful to recall that StreamCast and Grokster make money by selling advertising space, by directing ads to the screens of computers employing their software. As the record shows, the more the software is used, the more ads are sent out and the greater the advertising revenue becomes. Since the extent of the software's use determines the gain to the distributors, the commercial sense of their

[12] Of course, in the absence of other evidence of intent, a court would be unable to find contributory infringement liability merely based on a failure to take affirmative steps to prevent infringement, if the device otherwise was capable of substantial noninfringing uses. Such a holding would tread too close to the *Sony* safe harbor.

enterprise turns on high-volume use, which the record shows is infringing.[13] This evidence alone would not justify an inference of unlawful intent, but viewed in the context of the entire record its import is clear.

The unlawful objective is unmistakable.

B

In addition to intent to bring about infringement and distribution of a device suitable for infringing use, the inducement theory of course requires evidence of actual infringement by recipients of the device, the software in this case. As the account of the facts indicates, there is evidence of infringement on a gigantic scale, and there is no serious issue of the adequacy of MGM's showing on this point in order to survive the companies' summary judgment requests. Although an exact calculation of infringing use, as a basis for a claim of damages, is subject to dispute, there is no question that the summary judgment evidence is at least adequate to entitle MGM to go forward with claims for damages and equitable relief.

* * *

In sum, this case is significantly different from *Sony* and reliance on that case to rule in favor of StreamCast and Grokster was error. *Sony* dealt with a claim of liability based solely on distributing a product with alternative lawful and unlawful uses, with knowledge that some users would follow the unlawful course. The case struck a balance between the interests of protection and innovation by holding that the product's capability of substantial lawful employment should bar the imputation of fault and consequent secondary liability for the unlawful acts of others.

MGM's evidence in this case most obviously addresses a different basis of liability for distributing a product open to alternative uses. Here, evidence of the distributors' words and deeds going beyond distribution as such shows a purpose to cause and profit from third-party acts of copyright infringement. If liability for inducing infringement is ultimately found, it will not be on the basis of presuming or imputing fault, but from inferring a patently illegal objective from statements and actions showing what that objective was.

There is substantial evidence in MGM's favor on all elements of inducement, and summary judgment in favor of Grokster and StreamCast was error. On remand, reconsideration of MGM's motion for summary judgment will be in order….

[Ginsburg and Breyer concurrences omitted].

---

[13] Grokster and StreamCast contend that any theory of liability based on their conduct is not properly before this Court because the rulings in the trial and appellate courts dealt only with the present versions of their software, not "past acts ... that allegedly encouraged infringement or assisted ... known acts of infringement." This contention misapprehends the basis for their potential liability. It is not only that encouraging a particular consumer to infringe a copyright can give rise to secondary liability for the infringement that results. Inducement liability goes beyond that, and the distribution of a product can itself give rise to liability where evidence shows that the distributor intended and encouraged the product to be used to infringe. In such a case, the culpable act is not merely the encouragement of infringement but also the distribution of the tool intended for infringing use.

17 U.S.C. § 512. Limitations on liability relating to material online

(a) Transitory Digital Network Communications.— A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if—

(1) the transmission of the material was initiated by or at the direction of a person other than the service provider;
(2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;
(3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;
(4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and
(5) the material is transmitted through the system or network without modification of its content.

(b) System Caching.—

(1) Limitation on liability.— A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider in a case in which—

(A) the material is made available online by a person other than the service provider;
(B) the material is transmitted from the person described in subparagraph (A) through the system or network to a person other than the person described in subparagraph (A) at the direction of that other person; and
(C) the storage is carried out through an automatic technical process for the purpose of making the material available to users of the system or network who, after the material is transmitted as described in subparagraph (B), request access to the material from the person described in subparagraph (A),
if the conditions set forth in paragraph (2) are met.

(2) Conditions.— The conditions referred to in paragraph (1) are that—

(A) the material described in paragraph (1) is transmitted to the subsequent users described in paragraph (1)(C) without

modification to its content from the manner in which the material was transmitted from the person described in paragraph (1)(A);
(B) the service provider described in paragraph (1) complies with rules concerning the refreshing, reloading, or other updating of the material when specified by the person making the material available online in accordance with a generally accepted industry standard data communications protocol for the system or network through which that person makes the material available, except that this subparagraph applies only if those rules are not used by the person described in paragraph (1)(A) to prevent or unreasonably impair the intermediate storage to which this subsection applies;
(C) the service provider does not interfere with the ability of technology associated with the material to return to the person described in paragraph (1)(A) the information that would have been available to that person if the material had been obtained by the subsequent users described in paragraph (1)(C) directly from that person, except that this subparagraph applies only if that technology—

(i) does not significantly interfere with the performance of the provider's system or network or with the intermediate storage of the material;
(ii) is consistent with generally accepted industry standard communications protocols; and
(iii) does not extract information from the provider's system or network other than the information that would have been available to the person described in paragraph (1)(A) if the subsequent users had gained access to the material directly from that person;

(D) if the person described in paragraph (1)(A) has in effect a condition that a person must meet prior to having access to the material, such as a condition based on payment of a fee or provision of a password or other information, the service provider permits access to the stored material in significant part only to users of its system or network that have met those conditions and only in accordance with those conditions; and
(E) if the person described in paragraph (1)(A) makes that material available online without the authorization of the copyright owner of the material, the service provider responds expeditiously to remove, or disable access to, the material that is claimed to be infringing upon notification of claimed infringement as described in subsection (c)(3), except that this subparagraph applies only if—

(i) the material has previously been removed from the originating site or access to it has been disabled, or a court has ordered that the material be removed from the originating site or that access to the

material on the originating site be disabled; and
(ii) the party giving the notification includes in the notification a statement confirming that the material has been removed from the originating site or access to it has been disabled or that a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled.

(c) Information Residing on Systems or Networks At Direction of Users.—

(1) In general.— A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider—

(A)
(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
(ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
(iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;
(B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and
(C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.

(2) Designated agent.— The limitations on liability established in this subsection apply to a service provider only if the service provider has designated an agent to receive notifications of claimed infringement described in paragraph (3), by making available through its service, including on its website in a location accessible to the public, and by providing to the Copyright Office, substantially the following information:

(A) the name, address, phone number, and electronic mail address of the agent.
(B) other contact information which the Register of Copyrights may deem appropriate.
The Register of Copyrights shall maintain a current directory of agents available to the public for inspection, including through the Internet, in both electronic and hard copy formats, and may require payment of a fee by service providers to cover the costs of maintaining the directory.

(3) Elements of notification.—

(A) To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following:

(i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.

(iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.

(iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.

(v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.

(vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(B)

(i) Subject to clause (ii), a notification from a copyright owner or from a person authorized to act on behalf of the copyright owner that fails to comply substantially with the provisions of subparagraph (A) shall not be considered under paragraph (1)(A) in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent.

(ii) In a case in which the notification that is provided to the service provider's designated agent fails to comply substantially with all the provisions of subparagraph (A) but substantially complies with

clauses (ii), (iii), and (iv) of subparagraph (A), clause (i) of this subparagraph applies only if the service provider promptly attempts to contact the person making the notification or takes other reasonable steps to assist in the receipt of notification that substantially complies with all the provisions of subparagraph (A).

(d) Information Location Tools.— A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link, if the service provider—

(1)

(A) does not have actual knowledge that the material or activity is infringing;

(B) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(C) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(2) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

(3) upon notification of claimed infringement as described in subsection (c)(3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity, except that, for purposes of this paragraph, the information described in subsection (c)(3)(A)(iii) shall be identification of the reference or link, to material or activity claimed to be infringing, that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate that reference or link.

(e) Limitation on Liability of Nonprofit Educational Institutions.—

(1) When a public or other nonprofit institution of higher education is a service provider, and when a faculty member or graduate student who is an employee of such institution is performing a teaching or research function, for the purposes of subsections (a) and (b) such faculty member or graduate student shall be considered to be a person other than the institution, and for the purposes of subsections (c) and (d) such faculty member's or graduate student's knowledge or awareness of his or her infringing activities shall not be attributed to the institution, if—

(A) such faculty member's or graduate student's infringing activities do not involve the provision of online access to instructional materials that are or were required or recommended, within the preceding 3-year period, for a course taught at the institution by such faculty member or graduate student;

(B) the institution has not, within the preceding 3-year period, received more than two notifications described in subsection (c)(3) of claimed infringement by such faculty member or graduate student, and such notifications of claimed infringement were not actionable under subsection (f); and

(C) the institution provides to all users of its system or network informational materials that accurately describe, and promote compliance with, the laws of the United States relating to copyright.

(2) For the purposes of this subsection, the limitations on injunctive relief contained in subsections (j)(2) and (j)(3), but not those in (j)(1), shall apply.

(f) Misrepresentations.— Any person who knowingly materially misrepresents under this section—

(1) that material or activity is infringing, or

(2) that material or activity was removed or disabled by mistake or misidentification,

shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it.

(g) Replacement of Removed or Disabled Material and Limitation on Other Liability.—

(1) No liability for taking down generally.— Subject to paragraph (2), a service provider shall not be liable to any person for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing.

(2) Exception.— Paragraph (1) shall not apply with respect to material residing at the direction of a subscriber of the service provider on a system or network controlled or operated by or for the service provider that is removed, or to which access is disabled by the service provider, pursuant to a notice provided under subsection (c)(1)(C), unless the service provider—

(A) takes reasonable steps promptly to notify the subscriber that it has removed or disabled access to the material;

(B) upon receipt of a counter notification described in paragraph (3), promptly provides the person who provided the notification under subsection (c)(1)(C) with a copy of the counter notification, and informs that person that it will replace the removed material or cease disabling access to it in 10 business days; and

(C) replaces the removed material and ceases disabling access to it not less than 10, nor more than 14, business days following receipt

of the counter notice, unless its designated agent first receives notice from the person who submitted the notification under subsection (c)(1)(C) that such person has filed an action seeking a court order to restrain the subscriber from engaging in infringing activity relating to the material on the service provider's system or network.

(3) Contents of counter notification.— To be effective under this subsection, a counter notification must be a written communication provided to the service provider's designated agent that includes substantially the following:

(A) A physical or electronic signature of the subscriber.

(B) Identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before it was removed or access to it was disabled.

(C) A statement under penalty of perjury that the subscriber has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material to be removed or disabled.

(D) The subscriber's name, address, and telephone number, and a statement that the subscriber consents to the jurisdiction of Federal District Court for the judicial district in which the address is located, or if the subscriber's address is outside of the United States, for any judicial district in which the service provider may be found, and that the subscriber will accept service of process from the person who provided notification under subsection (c)(1)(C) or an agent of such person.

(4) Limitation on other liability.— A service provider's compliance with paragraph (2) shall not subject the service provider to liability for copyright infringement with respect to the material identified in the notice provided under subsection (c)(1)(C).

(h) Subpoena To Identify Infringer.—

(1) Request.— A copyright owner or a person authorized to act on the owner's behalf may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer in accordance with this subsection.

(2) Contents of request.— The request may be made by filing with the clerk—

(A) a copy of a notification described in subsection (c)(3)(A);

(B) a proposed subpoena; and

(C) a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title.

(3) Contents of subpoena.— The subpoena shall authorize and order the service provider receiving the notification and the subpoena to expeditiously disclose to

the copyright owner or person authorized by the copyright owner information sufficient to identify the alleged infringer of the material described in the notification to the extent such information is available to the service provider.
(4) Basis for granting subpoena.— If the notification filed satisfies the provisions of subsection (c)(3)(A), the proposed subpoena is in proper form, and the accompanying declaration is properly executed, the clerk shall expeditiously issue and sign the proposed subpoena and return it to the requester for delivery to the service provider.
(5) Actions of service provider receiving subpoena.— Upon receipt of the issued subpoena, either accompanying or subsequent to the receipt of a notification described in subsection (c)(3)(A), the service provider shall expeditiously disclose to the copyright owner or person authorized by the copyright owner the information required by the subpoena, notwithstanding any other provision of law and regardless of whether the service provider responds to the notification.
(6) Rules applicable to subpoena.— Unless otherwise provided by this section or by applicable rules of the court, the procedure for issuance and delivery of the subpoena, and the remedies for noncompliance with the subpoena, shall be governed to the greatest extent practicable by those provisions of the Federal Rules of Civil Procedure governing the issuance, service, and enforcement of a subpoena duces tecum.

(i) Conditions for Eligibility.—

(1) Accommodation of technology.— The limitations on liability established by this section shall apply to a service provider only if the service provider—

(A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers; and

(B) accommodates and does not interfere with standard technical measures.

(2) Definition.— As used in this subsection, the term "standard technical measures" means technical measures that are used by copyright owners to identify or protect copyrighted works and—

(A) have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process;

(B) are available to any person on reasonable and nondiscriminatory terms; and

(C) do not impose substantial costs on service providers or substantial burdens on their systems or networks.

(j) Injunctions.— The following rules shall apply in the case of any application for an injunction under section 502 against a service provider that is not subject to monetary remedies under this section:

(1) Scope of relief.—

(A) With respect to conduct other than that which qualifies for the limitation on remedies set forth in subsection (a), the court may grant injunctive relief with respect to a service provider only in one or more of the following forms:

(i) An order restraining the service provider from providing access to infringing material or activity residing at a particular online site on the provider's system or network.

(ii) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is engaging in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.

(iii) Such other injunctive relief as the court may consider necessary to prevent or restrain infringement of copyrighted material specified in the order of the court at a particular online location, if such relief is the least burdensome to the service provider among the forms of relief comparably effective for that purpose.

(B) If the service provider qualifies for the limitation on remedies described in subsection (a), the court may only grant injunctive relief in one or both of the following forms:

(i) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is using the provider's service to engage in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.

(ii) An order restraining the service provider from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States.

(2) Considerations.— The court, in considering the relevant criteria for injunctive relief under applicable law, shall consider—

(A) whether such an injunction, either alone or in combination with other such injunctions issued against the same service provider under this subsection, would significantly burden either the provider or the operation of the provider's system or network;

(B) the magnitude of the harm likely to be suffered by the copyright owner in the digital network environment if steps are not taken to prevent or restrain the infringement;
(C) whether implementation of such an injunction would be technically feasible and effective, and would not interfere with access to noninfringing material at other online locations; and
(D) whether other less burdensome and comparably effective means of preventing or restraining access to the infringing material are available.

(3) Notice and ex parte orders.— Injunctive relief under this subsection shall be available only after notice to the service provider and an opportunity for the service provider to appear are provided, except for orders ensuring the preservation of evidence or other orders having no material adverse effect on the operation of the service provider's communications network.

(k) Definitions.—

(1) Service provider.—
(A) As used in subsection (a), the term "service provider" means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.
(B) As used in this section, other than subsection (a), the term "service provider" means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A).
(2) Monetary relief.— As used in this section, the term "monetary relief" means damages, costs, attorneys' fees, and any other form of monetary payment.

(l) Other Defenses Not Affected.— The failure of a service provider's conduct to qualify for limitation of liability under this section shall not bear adversely upon the consideration of a defense by the service provider that the service provider's conduct is not infringing under this title or any other defense.

(m) Protection of Privacy.— Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on—

(1) a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i); or
(2) a service provider gaining access to, removing, or disabling access to material in cases in which such conduct is prohibited by law.

(n) Construction.— Subsections (a), (b), (c), and (d) describe separate and distinct functions for purposes of applying this section. Whether a service provider qualifies for the limitation on liability in any one of those subsections shall be based solely on the criteria in that subsection,

and shall not affect a determination of whether that service provider qualifies for the limitations on liability under any other such subsection.

Io Group, Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132 (N.D. Cal. 2008).
Lloyd, Magistrate Judge.

…I. BACKGROUND…

A. The Parties

Plaintiff Io Group, Inc. ("Io"), doing business as Titan Media, produces, markets and distributes a variety of adult entertainment products, including audiovisual works. It holds and owns a number of registered copyrights for its films.

Defendant Veoh Networks, Inc. ("Veoh") is a self-described "Internet Television Network," which provides software and a website (veoh.com) that enables the sharing of user-provided video content over the Internet-from job interviews, to family gatherings, to films by aspiring filmmakers. Since its website launch in February 2006, users have uploaded and shared hundreds of thousands of videos on Veoh. Veoh says that it has received notices of alleged copyright infringement with respect to less than seven percent of those videos.

In addition to user-submitted content, users may also access videos from Veoh's content partners, including Turner, CBS, Us Magazine, Road and Track Magazine, Car and Driver Magazine, and United Talent Agency. Veoh itself creates and uploads promotional videos to its system. And, in some instances, Veoh's content partners have given video files to Veoh, in which case Veoh's employees upload those files on their behalf. There is no allegation that Veoh employees have submitted and uploaded infringing content to veoh.com; and, the only content in question here is material that was submitted to Veoh by its users.

Once video files are uploaded to Veoh's system, Veoh's employees can and do select videos to be featured on the "Featured Videos" portion of Veoh's website.

Veoh now offers advertising opportunities and participates in certain Google-sponsored ad programs. Additionally, Veoh has implemented a "premium content" program in which users who upload content may choose to charge for viewing the content, and Veoh receives a portion of the proceeds. However, during the time period encompassed by the complaint, Veoh did not charge users for viewing videos, or impose any membership or subscription fee. Also, there was no advertising on Veoh.

B. Alleged Infringement

Between June 1, 2006 and June 22, 2006, Io says it discovered that clips from ten of its copyrighted films had been uploaded and viewed on veoh.com without its authorization. Several of the allegedly infringing video files are less than one minute long, and some were less than six seconds in length. A couple of files were longer than 20 minutes; and, at oral argument, plaintiff's counsel clarified that, in some instances, there was a series of six-second clips for a particular work (or, on average, about 20 minutes of clips per movie). He further represented that the longest clip is about 40 minutes long. However, none of the clips contained copyright

notices, save for one work that displayed the Titan Media trademark several minutes into the clip.

When it discovered the presence of the allegedly infringing files, Io did not tell Veoh that it believed its copyrights were being violated. Veoh's first notice of the claimed infringement was Io's filing of the instant lawsuit on June 23, 2006. Coincidentally, Veoh had already independently decided that it would no longer permit adult content on veoh.com. By the time this suit was filed, access to all adult content on Veoh's website—including any content allegedly infringing Io's copyrights—had been terminated.

C. Veoh's Policies

Veoh has established Terms of Use and Acceptable Use policies, which are posted on its website. Before users can upload video content to veoh.com, they must register with Veoh and agree to abide by those policies. During the relevant period of time encompassed by the complaint, Veoh's Terms of Use required users to agree that:

> any User Material that you make available to the Veoh Service may be made freely available by Veoh through the Veoh Service, including without limitation for download by other users, and that this permission is made and granted in consideration of your use of the Veoh Service and is nonexclusive, perpetual, royalty-free, irrevocable and transferable.

The Terms of Use further advised:

> Veoh shall have no obligation to monitor any User Material. However, Veoh and its agents shall have and do reserve the right to monitor any User Material from time to time for any lawful purpose. Veoh may, without notice to you, remove or block content of any User Material from the Veoh Service, including disabling access to such User material that you have downloaded through the Veoh Service. Veoh reserves the right to terminate your use of the Veoh Service if we determine that you have violated these Terms or the Acceptable Use Policy.
>
> Veoh requires all users of the Veoh Service to comply with copyright and other intellectual property laws. Accordingly, you may not publish or make available any User Material that constitutes an infringement of third party intellectual property rights, including rights granted by U.S. copyright law, or that otherwise violates the Acceptable Use Policy. You represent and warrant that you have all rights necessary to publish and distribute any User Material made available by you through the Veoh Service and that such User Material conforms to the Acceptable Use Policy. You agree to indemnify and hold Veoh harmless from and against any liability, claims, losses, demands or damages arising out of or relating to your violation of these Terms or the Acceptable Use Policy.
>
> As explained above, Veoh does not permit copyright infringing activities on the Veoh Service and reserves the right to terminate access to the Veoh Service, and

> remove all User Materials posted, by any persons who are found to be repeat infringers (i.e., persons found to have uploaded copyright infringing User Material on more than two occasions).

Similarly, Veoh's Acceptable Use Policy advised users that:

> Veoh respects the rights of copyright owners to control commercial uses of their material, and expects our users to do the same. You are responsible for complying with all federal and state laws applicable to the content available through the Veoh Services, including copyright laws.
>
> Accordingly, Veoh reserves the right to terminate the service account of anyone who it learns is using the Veoh Services in violation of copyright law.

Veoh also reminds users of its policies during the upload process. When a user now begins to upload a video, the system displays a message stating, "Do not upload copyrighted, pornographic, obscene, violent, or any other videos that violate Veoh Publisher Terms and Conditions." Veoh says that it gave a substantially similar warning (presumably without the reference to pornographic material) to users during the relevant period encompassed by the complaint.

Veoh has a designated Copyright Agent to receive notification of claimed violations and provides information about how and where to send notices of claimed infringement. When Veoh receives notice that a user has uploaded infringing content after a first warning, then the user's account is terminated, all content provided by that user is disabled (unless the content was also published by another non-terminated user and is not the subject of a DMCA notice), and the user's email address is blocked so that a new account cannot be opened with that same address. Veoh also has the ability to disable access to such material on its users' hard drives (assuming their computers are still connected to the Internet). Additionally, Veoh has adopted means for generating a digital "fingerprint" for each video file, which enables Veoh to terminate access to any other identical files and prevent additional identical files from ever being uploaded by any user.

D. Uploading Video Content on Veoh.com

1. User-Submitted Videos

As noted above, users must register with Veoh before they can upload video content to the website. In the registration process, users are required to provide a user name, an email address and a password. They may, but are not required to, give their actual names.

When users upload a video file to Veoh's system, they are asked to (a) provide a title and description; (b) enter key words or "tags"; (c) select up to four categories which best describe the video; and (d) select a content rating. Users then select the video file (from wherever it resides on their computers) and upload it to the Veoh system.

When the Veoh system receives a video submission, its computers first confirm that the submitted file is, in fact, a video file with a compatible "codec" (or compression format). If the submission is a compatible video file, the Veoh system automatically extracts certain metadata from it (e.g., file format and length), assigns a unique video identification number to it, indexes the user-entered information and stores the information in a database on Veoh's servers. Users can then conduct searches (e.g., by title, description, genre, etc.) of the database in order to find videos they wish to view. The database also automatically indexes video files into a series of lists, such as "Most Recent;" "Top Rated," "Most Popular," "Most Discussed" and "Top Favorite."

2. "Flash" Files and Screencaps[5]

As part of the uploading process, when Veoh receives a video file from a user, its system also automatically (a) converts each user-submitted video into Flash format; and (b) extracts several still images from each file.

a. Flash Files

Users submit video files in a variety of formats. A "bit-for-bit" equivalent of the user-submitted video resides on Veoh's servers indefinitely in its original format. If users download Veoh's "Veoh Client" software, then they may download a copy of the video file in its original format to their computer hard drive.

Veoh says that the vast majority of Internet users now have software that can play videos in "Flash" format. So, as part of the uploading process, when the Veoh system receives a user-submitted video, its computers use third-party software to automatically convert each user-submitted video into Flash format. Veoh selects certain parameters (e.g., frame rate, bit rate and frame size) which it says are default values within a range of parameters set by the third party software used in the process. The creation of the Flash files is entirely automated.

Before October 2006, and during the period of time encompassed by the complaint, videos that were shorter than ten minutes in length would be converted into Flash format. For videos longer than ten minutes, the Veoh system would create a three-minute Flash preview clip. Since October 2006, Veoh's system has converted all video files to Flash format without limitation as to length.

b. Screencaps

During the upload process, Veoh's system also automatically extracts several still images from each file—i.e., 16 full resolution screen captures, or "screencaps," in the same resolution as the incoming video and 16 lower resolution screencaps. Screencaps in the original video resolution reside on the Veoh system but are not available for users to view or access.

Of the 16 lower-resolution images, one is used to represent the video in a search result. Thus, when users search for videos on Veoh, the search results are shown in a grid, with each result represented by a still image extracted from a video. When users click on a specific image on the

[5] Defendant refers to the still-image screen captures as thumbnails. Plaintiff disputes whether all of the still images are true thumbnails, or reduced-size screenshots. This court does not find the discrepancy to be material. For present purposes, it will simply refer to these images as still images or screencaps.

search results page, they see a “Video Details Page” containing the video and a link called “Video Screencaps.” By clicking on the “Video Screencaps” link, users can see the 16 lower-resolution screenshots from the video. Veoh says that the screencaps help users understand what a video likely contains before they download it. However, it acknowledges that the value of the screencaps was diminished by the advent of Flash previews on Veoh. The creation of the screencaps is entirely automated.

3. Post-Publication “Spot Check”
Veoh employees occasionally “spot check” videos after publication for compliance with Veoh’s policies and to ensure accuracy in the description and categorization of the content. For example, Veoh has, on occasion, edited the video description field. And, when adult content was still permitted on veoh.com, Veoh employees sometimes reviewed files to ensure proper ratings on any file containing sexually explicit material and reviewed sexually explicit files to determine whether they should be identified as “gay” or “straight” and added tags as needed. Additionally, if a “spot check” reveals an instance of blatant copyright infringement, Veoh disables access to such material. For example, Veoh has, in at least one instance, removed videos of a movie known to have been released in only theaters.

Veoh’s policies previously stated that all video content was approved by editors; and, the record indicates that Veoh’s employees may have watched the first ten videos submitted to veoh.com by users. However, Veoh claims that the policy was never implemented because it was not feasible to do so given the number of user submissions that have since been made….

III. DISCUSSION

Ordinarily, issues concerning liability would be examined before determining whether any safe harbor applies. However, while the DMCA safe harbors do not immunize online service providers from liability, they provide copyright owners with only limited injunctive relief. Under the circumstances presented here, the court finds it appropriate and more efficient to first address Veoh’s motion as to the applicability of the safe harbor under DMCA section 512(c).

As discussed more fully below, even assuming that plaintiff’s infringement claims pass summary judgment muster, this court concludes that Veoh is eligible for safe harbor protection from damages and, further, that the limited injunctive relief provided under the DMCA is moot.

A. The DMCA

Enacted in 1998, the DMCA was “designed to facilitate the robust development and world-wide expansion of electronic commerce, communications, research, development, and education in the digital age.” S.Rep. No. 105-190, at 1-2 (1998). “Difficult and controversial questions of copyright liability in the online world prompted Congress to enact Title II of the DMCA, the Online Copyright Infringement Liability Limitation Act (OCILLA).” In order to strike a balance between their respective interests, OCILLA seeks to “preserve[ ] strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment.” S. Rep. 105-190, at 20 (1998); H.R. Rep. 105-551(II), at 49 (1998). “Congress hoped to provide ‘greater certainty to service providers

concerning their legal exposure for infringements that may occur in the course of their activities.'"

OCILLA enables qualifying service providers to limit their liability for claimed copyright infringement under four "safe harbors." "These safe harbors provide protection from liability for: (1) transitory digital network communications; (2) system caching; (3) information residing on systems or networks at the direction of users; and (4) information location tools." "These safe harbors limit liability but 'do not affect the question of ultimate liability under the various doctrines of direct, vicarious, and contributory liability.'" That is, they protect qualifying service providers from liability for all monetary relief for direct, vicarious and contributory infringement, leaving copyright owners with limited injunctive relief. Further, the safe harbor provisions are not exclusive of any other defense an accused infringer might have. "Far short of adopting enhanced or wholly new standards to evaluate claims of copyright infringement against online service providers, Congress provided that OCILLA's 'limitations of liability apply if the provider is found to be liable under existing principles of law.'"

With these principles in mind, the court now considers whether Veoh is entitled to safe harbor with respect to the alleged infringing activity here.

B. DMCA Threshold Requirements

To avail itself of any of the four safe harbors, Veoh must first satisfy certain threshold requirements. That is, it must be a "service provider" and it must adopt, reasonably implement and inform subscribers of a policy providing that it may, in appropriate circumstances, terminate the accounts of repeat infringers. Further, the service provider is obliged to accommodate, and must not interfere with, "standard technical measures" used by copyright owners to identify or protect copyrighted works.

Io does not dispute that Veoh is a "service provider" as defined by DMCA Section 512(k)(1)(B). Nor does it dispute that Veoh (a) has adopted and informed account holders of its repeat infringer policy and (b) accommodates, and does not interfere with, "standard technical measures" used to protect copyrighted works. However, Io contends that there is a triable issue whether Veoh implements its repeat infringer policy in a reasonable manner.

The DMCA does not say what "reasonably implemented" means. Nonetheless, the Ninth Circuit has held that "a service provider 'implements' a policy if it has a working notification system, a procedure for dealing with DMCA-compliant notifications, and if it does not actively prevent copyright owners from collecting information needed to issue such notifications." "The statute permits service providers to implement a variety of procedures, but an implementation is reasonable if, under 'appropriate circumstances,' the service provider terminates users who repeatedly or blatantly infringe copyright."

As discussed above, Veoh's evidence indicates that it has a working notification system and a procedure for dealing with copyright infringement notices:

• Since at least April 2006, and at all times encompassed by the complaint, Veoh's policies have identified its designated Copyright Agent to receive notification of claimed violations and provide information about how and where to send notices of claimed infringement.

• Veoh often responds to infringement notices the same day they are received, or at most, within a few days.

• When Veoh receives notice that a user has uploaded infringing content after a first warning, then the account is terminated, all content provided by that user is disabled (unless the content was also published by another non-terminated user and is not the subject of a DMCA notice), and the user's email address is blocked so that a new account cannot be opened with that same address.

• Veoh has adopted means for generating a "hash," or digital "fingerprint," for each video file. This technology essentially enables Veoh to terminate access to any other identical files and prevent additional identical files from ever being uploaded by any user.

Veoh asserts that, since its website was launched, it has terminated 1,096 users for repeat copyright violations. Plaintiff has presented no evidence to the contrary; and, there is no suggestion in the record before the court that Veoh actively prevents copyright owners from collecting information needed to issue notification of claimed copyright violations.

Io nevertheless contends that Veoh's policy fails because it does not prevent repeat infringers from reappearing on Veoh under a pseudonym and a different email address. At one time, Veoh apparently attempted to verify a user's email address by sending a confirming email message before allowing that user to upload video files to veoh.com. However, Veoh says that practice was discontinued as "an error-prone process." Io agrees that Veoh is not obliged to locate repeat infringers, but argues that there is no way for Veoh to discover if a disingenuous user has, in fact, reappeared with a new account. Here, Io points out that its vice president, Keith Ruoff, was able to obtain a new Veoh account using the pseudonym "FauxUser99" and the email address "Faux User 01@ yahoo.com"—an address which he says he acquired from Yahoo! using the pseudonym "John Doe." In essence, Io contends that Veoh fails to reasonably track repeat infringers and that its repeat infringer policy is tantamount to no policy at all. This court disagrees.

With respect to the reasonableness of a service provider's implementation, the Ninth Circuit has explained:

> A service provider reasonably implements its repeat infringer policy if it terminates users "when appropriate." Section 512(i) itself does not clarify when it is "appropriate" for service providers to act. It only requires that a service provider terminate users who are "repeat infringers."
>
> *To identify and terminate repeat infringers, a service provider need not affirmatively police its users for evidence of repeat infringement.* Section 512(c) states that "[a] service provider shall not be liable for monetary relief" if it does

> not know of infringement. A service provider is also not liable under § 512(c) if it acts "expeditiously to remove, or disable access to, the material" when it (1) has actual knowledge, (2) is aware of facts or circumstances from which infringing activity is apparent, or (3) has received notification of claimed infringement meeting the requirements of § 512(c)(3). Were we to require service providers to terminate users under circumstances other than those specified in § 512(c), § 512(c)'s grant of immunity would be meaningless. This interpretation of the statute is supported by legislative history. See H.R. Rep., at 61 (Section 512(i) is not intended "to undermine the ... knowledge standard of [§ 512](c).").

(emphasis added).

Moreover, the hypothetical possibility that a rogue user might reappear under a different user name and identity does not raise a genuine fact issue as to the implementation of Veoh's policy. In *Corbis*, plaintiff alleged that Amazon failed to reasonably implement its repeat infringer policy because it did not prevent a prior infringer from reappearing on one of Amazon's retail platforms under different names. Observing that the DMCA requires reasonable, not perfect, policies, the court held that "[t]he mere fact that [the repeat infringer] appeared on zShops under a different user name and identity does not, by itself, create a legitimate question of fact regarding the procedural implementation of Amazon's termination policy." There, plaintiff presented no evidence that Amazon intentionally allowed the repeat infringer to open new accounts. Nor did plaintiff suggest that a more effective and reasonable means of denying the repeat infringer's access could have been implemented by Amazon.

Here, Io has presented no evidence that a repeat infringer has, in fact, established a new account under false pretenses, much less that Veoh has intentionally allowed that to happen. Its supposition about the hypothetical possibility that a repeat infringer may have done so is not evidence. There is no indication that Mr. Ruoff is a repeat infringer who should have been blocked; and, the fact that he was able to open a second account does not give rise to a genuine issue of material fact as to the reasonableness of Veoh's implementation.

Citing to an unpublished decision from this district, A & M Records, Inc. v. Napster, Inc., 2000 WL 573136, (N.D. Cal., May 12, 2000), Io contends that, in order to satisfy section 512(i), Veoh must be required to track users by their actual names or by Internet Protocol ("IP") addresses. That decision is readily distinguishable. There, the court found a triable issue as to whether Napster reasonably implemented its repeat infringer policy because plaintiff submitted evidence that Napster was not only capable of blocking IP addresses, but had in fact done so for certain users.

Here, Io has presented no evidence suggesting that tracking (or verifying) users' actual identity or that blocking their IP addresses is a more effective reasonable means of implementation. There is no material dispute that, while IP addresses identify a particular computer connected to the Internet, they do not distinguish between users (e.g., family members) who may share the same computer. See generally Columbia Ins. Co. v. seescandy.com, 185 F.R.D. 573, 575 (N.D.

Cal. 1999) (IP addresses "are a series of numbers that are used to specify the address of a particular *machine* connected to the Internet.") (emphasis added).[8]

More to the point, section 512(i) does not require service providers to track users in a particular way to or affirmatively police users for evidence of repeat infringement. Instead, "[a] policy is unreasonable only if the service provider failed to respond when it had knowledge of the infringement." Here, the uncontroverted evidence shows that Veoh (a) has a working notification system, (b) has a procedure for dealing with DMCA-compliant notifications, and (c) does not actively prevent copyright owners from collecting information necessary to issue such notices. Plaintiff says that defendant does not qualify for safe harbor because it does not track infringers. However, Veoh does track content that has been identified as infringing and permanently blocks that content from ever being uploaded by any user.

Accordingly, the court finds that Veoh has presented evidence that it satisfies the threshold requirements to qualify for safe harbor under the DMCA. Plaintiff has not presented evidence raising a genuine issue of material fact as to whether Veoh implements its repeat infringer policy in a reasonable manner.

The court now turns to the question whether Veoh qualifies for safe harbor under Section 512(c).

C. DMCA Section 512(c) Safe Harbor

DMCA Section 512(c) limits a service provider's liability "for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider." A service provider that meets the threshold conditions of Section 512(i) then qualifies for safe harbor under Section 512(c) if it:

> (A) (i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
>
> (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
>
> (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;
>
> (B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and
>
> (C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.

[8] The court takes judicial notice of the Wikipedia definition of "IP address" as to the fact that an IP address may be shared by multiple users. This is not a matter that is subject to reasonable dispute.

In essence, a service provider is eligible for safe harbor under section 512(c) if it (1) does not know of infringement; or (2) acts expeditiously to remove or disable access to the material when it (a) has actual knowledge, (b) is aware of facts or circumstances from which infringing activity is apparent, or (c) has received DMCA-compliant notice; and (3) either does not have the right and ability to control the infringing activity, or—if it does—that it does not receive a financial benefit directly attributable to the infringing activity.

According to plaintiff, Veoh does not qualify for safe harbor under Section 512(c) because (a) the materials in question were not stored on Veoh's system at the direction of a user; (b) Veoh was aware of apparent infringing activity; and (c) Veoh has the right and ability to control the infringing activity and obtains a direct financial benefit from such activities. The court will address each of these contentions in turn.

1. "At the Direction of a User"
As stated above, section 512(c) provides safe harbor "for infringement of a copyright by reason of the storage at the direction of a user of material" residing on a service provider's system or network. The legislative history indicates that such storage includes, by way of example, "providing server space for a user's web site, for a chatroom, or other forum in which material may be posted at the direction of users." Excluded from Section 512(c)'s safe harbor is "material 'that resides on the system or network operated by or for the service provider through its own acts or decisions and not at the direction of a user.'"

Plaintiff contends that the Flash files and screencaps created during the publication process are not stored on Veoh's system "at the direction of a user," but by Veoh's own acts and decisions. Here, it asserts that users do not themselves create or possess the Flash and still-image files when they upload videos to Veoh's system. It further contends that, by agreeing that Veoh may make their videos freely available on its website, users never instruct or direct Veoh to create these files, except in the broadest possible sense. Io argues that Section 512(c) was not intended to protect the creation (automated or not) of these files because Veoh uses them as a means of distribution (e.g., by indexing content and organizing them into lists), and not just storage.

Defendant does not deny that, using third-party software, its system creates the Flash and still-image files from user-submitted content. Nonetheless, Veoh maintains that these files are the result of an automated encoding process initiated entirely at the volition of users when they upload video files. Veoh maintains that it falls within the Section 512(c) safe harbor because the Flash and still-image files are used to facilitate access to content submitted to its website.

There is no apparent dispute as to the material facts—only as to the conclusions to be drawn from them. Essentially, the issue is whether Veoh is disqualified from Section 512(c)'s safe harbor because of automated functions that facilitate access to user-submitted content on its website. In the context of Veoh's business, this appears to be a matter of first impression. Based on the record presented, this court concludes that Veoh is not disqualified from Section 512(c) safe harbor on this basis.

To begin, the structure and language of OCILLA indicate that service providers seeking safe harbor under Section 512(c) are not limited to merely storing material. The statute itself is

structured in a way that distinguishes between so-called "conduit only" functions under Section 512(a) and those functions addressed by Section 512(c) (and other subsections as well). Perhaps most notably, OCILLA contains two definitions of "service provider." The narrower definition, which pertains only to service providers falling under Section 512(a), "means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, *without modification to the content of the material as sent or received*."

By contrast, no such limitation as to the modification of material is included in the broader definition of "service provider," which the parties agree applies to Veoh. Instead, "the term 'service provider' means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A)." Had Congress intended to include a limitation as to a service provider's modification of user-submitted information, it would have said so expressly and unambiguously.

Moreover, caselaw also supports the conclusion that Veoh is not precluded from safe harbor under Section 512(c) by virtue of its automated processing of user-submitted content. In at least one case, a service provider was not precluded from safe harbor even when its employees engaged in some review of submitted materials before posting them to defendant's website. In Costar Group, Inc. v. LoopNet, Inc., the defendant offered a service that enabled subscribers to upload real estate photos to a folder on the defendant's system. 164 F. Supp. 2d 688 (D. Md. 2001). Defendant's employees briefly reviewed the submitted photos and posted to the website only those that met defendant's criteria—that is, any photos that did not depict real estate or which obviously were copyrighted by a third-party would not be posted. The court held that defendant nonetheless satisfied the requirement that material be stored at the direction of a user. In essence, it concluded that the photos were uploaded, in the first instance, at the volition of users and that defendant's employees simply performed a "gateway" function that furthered the goals of the DMCA.

Here, Veoh has simply established a system whereby software automatically processes user-submitted content and recasts it in a format that is readily accessible to its users. Veoh preselects the software parameters for the process from a range of default values set by the third-party software. But Veoh does not itself actively participate or supervise the uploading of files. Nor does it preview or select the files before the upload is completed. Instead, video files are uploaded through an automated process which is initiated entirely at the volition of Veoh's users. See The Cartoon Network LP, LLP v. CSC Holdings, Inc., 536 F.3d 121, 131 (2d Cir. 2008) ("In determining who actually 'makes' a copy, a significant difference exists between making a request to a human employee, who then volitionally operates the copying system to make the copy, and issuing a command directly to a system, which automatically engages in no volitional conduct."). Inasmuch as this is a means of facilitating user access to material on its website, this court finds that Veoh does not lose safe harbor through the automated creation of these files. "[O]ne of the stated purposes of [the DMCA] was to 'facilitate the robust development and worldwide expansion of electronic commerce, communications, research, development, and education in the digital age.'"

2. Actual Knowledge of Infringing Activity

It is undisputed that, before it filed the instant action, plaintiff provided no notice to Veoh of any claimed copyright infringement. Thus, there is no question on the record presented that Veoh lacked actual knowledge of the alleged infringing activity at issue. See 17 U.S.C. § 512(c)(1)(A) and (C); see also Corbis Corp., 351 F. Supp. 2d at 1107 ("[Plaintiff's] decision to forego the DMCA notice provisions ... stripped it of the most powerful evidence of a service provider's knowledge-actual notice of infringement from the copyright holder.") (citation omitted).

3. Apparent Infringing Activity

Nonetheless, Io contends that Veoh was aware of several signs of apparent infringing activity. Under this so-called "red flag" test, a service provider may lose safe harbor "if it fails to take action with regard to infringing material when it is 'aware of facts or circumstances from which infringing activity is apparent.'" In determining whether a service provider has such awareness, "the question is not 'what a reasonable person would have deduced given all the circumstances.'" "Instead the question is whether the service provider deliberately proceeded in the face of blatant factors of which it was aware." In other words, "apparent knowledge requires evidence that a service provider 'turned a blind eye to 'red flags' of obvious infringement.'"

Io argues that there were several "red flags" of obvious infringement here. Io says that, under 17 U.S.C. § 205(c), its copyright registrations provided constructive knowledge as to its ownership of the works. Additionally, plaintiff says that it was obvious that the works in question were professionally created and, further, that one of them contained Io's trademark. In any event, Io maintains that the absence of labels required under 18 U.S.C. § 2257(f)(4) was a "red flag" that the uploading user did not have authority to submit the content in question.

However, none of the allegedly infringing video files uploaded by Veoh's users contained Io's copyright notices. Although one of the works did contain plaintiff's trademark several minutes into the clip, there is no evidence from which it can be inferred that Veoh was aware of, but chose to ignore, it. Nor is this court convinced that the professionally created nature of submitted content constitutes a per se "red flag" of infringement sufficient to impute the requisite level of knowledge or awareness to Veoh. Indeed, with the video equipment available to the general public today, there may be little, if any, distinction between "professional" and amateur productions.

Similarly unavailing are Io's arguments as to the sexually explicit nature of the works themselves. Io nevertheless contends that the absence of labels on the material in question under 18 U.S.C. § 2257 was a "red flag" of apparent copyright infringement. In essence, the statute to which Io refers—section 2257 of the Child Protection and Obscenity Enforcement Act of 1988—requires producers of sexually explicit material to maintain certain records as to the performers depicted and to label each such work with a statement indicating where those records are located. There is some indication in the record that Veoh generally was aware of this law. Io argues that Veoh therefore should have known that no legitimate producer of sexually explicit material would have omitted the requisite labels on the video clips in question.

Viewing the evidence in the light most favorable to plaintiff, it has, at best, raised a fact question as to whether Veoh was aware that federal labeling laws might have been violated. However, the matter before this court does not concern whether there was a violation of those laws. Under the

circumstances presented here, the absence of required labels does not give rise to a genuine issue of material fact as to whether Veoh had the requisite level of knowledge or awareness that plaintiff's copyrights were being violated. Even "[w]hen a website traffics in pictures that are titillating by nature" and describes them as "illegal" or "stolen," "[w]e do not place the burden of determining whether photographs are actually illegal on a service provider."

4. Acts Expeditiously to Remove or Disable Access to Material
Even assuming Veoh had sufficient knowledge or awareness of the allegedly infringing activity in question, Veoh would not lose safe harbor protection if it acted expeditiously to remove, or disable access to, the material. The instant action presents a somewhat unusual situation in that Veoh independently removed all adult content from its website before it received notice of any claimed copyright violations.

Nevertheless, undisputed evidence submitted by Veoh shows that when it receives DMCA-compliant notice of copyright infringement, it responds and removes noticed content as necessary on the same day the notice is received (or within a few days thereafter).

In addition to responding to DMCA notices, Veoh says that it also promptly investigates other complaints about content on its website. Here, Veoh points out that its website has a "Flag It!" feature that enables users to bring certain content to Veoh's attention by "flagging" it—that is, selecting from a set list of reasons (e.g., misrated content, sexually explicit content, obscene content, etc.). Plaintiff argues that Veoh has willfully blinded itself to facts suggesting infringement because the list of reasons on the "Flag It!" feature no longer contains a choice for "appears to contain copyrighted material." Yet, the "Flag It!" feature itself contains a notice, prominently displayed at the top of the "Flag It!" dialog box, directing copyright owners to a link with instructions for submitting a copyright infringement notice to Veoh.

In sum, there is no evidence raising a genuine issue of material fact that Veoh was aware of, but deliberately chose to ignore, "red flags" of infringement or that Veoh fails to act expeditiously to remove or disable access to infringing material upon obtaining knowledge or awareness of infringing activity.

5. Right and Ability to Control Infringing Activity
A service provider nonetheless loses the protection of Section 512(c)'s safe harbor where it (a) has the right and ability to control the infringing activity and (b) receives a financial benefit directly attributable to such activity. "Both elements must be met for the safe harbor to be denied." These requirements grew out of the common law standard for vicarious liability, and the Ninth Circuit has indicated that these elements under the DMCA are to be interpreted consistently with common law. See CCBill, 488 F.3d at 1117 ("[W]e hold that 'direct financial benefit' should be interpreted consistent with the similarly-worded common law standard for vicarious copyright liability."). For present purposes, even assuming (without deciding) that Veoh received a direct financial benefit from the alleged infringing activity, this court finds that defendant does not have the right and ability to control such activity.

As formulated by the Supreme Court, one "infringes vicariously by profiting from direct infringement while declining to exercise a right to stop or limit it." Metro-Goldwyn-Mayer

Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 930 (2005). "Thus, under Grokster, a defendant exercises control over a direct infringer when he has both a legal right to stop or limit the directly infringing conduct, as well as the practical ability to do so." Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1173 (9th Cir. 2007).

Plaintiff contends that elements of the requisite "right and ability to control" are present here because Veoh has established and enforced policies that prohibit users from engaging in a host of illegal and other conduct on its website-namely, policies which prohibit users from (a) violating the intellectual property rights of others, (b) making unsolicited offers, sending ads, proposals or junk mail, (c) impersonating other people, (d) misrepresenting sources of material, (e) harassing, abusing, defaming, threatening or defrauding others, (f) linking to password protected areas and (g) spidering material. Plaintiff emphasizes that Veoh exercises the right to police its system by conducting occasional "spot checks" of video files for compliance and that Veoh has enforced its policies by removing content and terminating offending accounts.

However, the plain language of section 512(c) indicates that the pertinent inquiry is not whether Veoh has the right and ability to control it system, but rather, whether it has the right and ability to control the infringing activity. Under the facts and circumstances presented here, the two are not one and the same.

To begin, the statute presupposes a service provider's control of its system or network. The safe harbor will be closed only to those service providers who, among other things, have the "right and ability to control" the "infringing activity."

Moreover, courts have held that the right and ability to control infringing activity, as the concept is used in the DMCA, cannot simply mean the ability of a service provider to block or remove access to materials posted on its website or stored on its system. Indeed, a contrary holding would render the DMCA internally inconsistent:

> The DMCA specifically requires a service provider to remove or block access to materials posted on its system when it receives notice of claimed infringement. The DMCA also provides that the limitations on liability only apply to a service provider that has adopted and reasonably implemented ... a policy that provides for the termination in appropriate circumstances of [users] of the service provider's system or network who are repeat infringers. Congress could not have intended for courts to hold that a service provider loses immunity under the safe harbor provision of the DMCA because it engages in acts that are specifically required by the DMCA.

Borrowing from patent infringement cases involving the intent requirement for contributory liability of trademark licensors, one court has concluded that, instead, "something more" is required.

Precisely what constitutes the requisite right and ability to control in the present context is somewhat hard to define, although this court is not without some guidance. At least one court has

observed that the requisite "right and ability to control" "presupposes some antecedent ability to limit or filter copyrighted material."

Such a conclusion does not appear to be inconsistent with precedent set in Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996) and A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001). In *Fonovisa*, the plaintiff owned copyrights and trademarks in certain music recordings. It claimed that the defendant, a swap meet proprietor, was liable for third-party vendors' sales of infringing counterfeit recordings. Sufficient elements of control were found where defendant had the right to terminate vendors for any reason, promoted the swap meet, and controlled customers' access to the swap meet area. Notably, there was no dispute that the defendant was aware that vendors were selling counterfeit recordings in violation of plaintiff's copyrights and trademarks. Indeed, it was alleged that the County Sheriff previously seized thousands of counterfeit recordings from the swap meet and notified the defendant that infringing sales continued. The defendant evidently agreed to provide the Sheriff with information about each vendor, but did not do so. In essence, the swap meet proprietor and the infringing vendors "were engaged in a mutual enterprise of infringement."

Fonovisa was extended to the online context in A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001). *Napster* concerned the Internet service infamous for its software that facilitated the transmission of copyrighted music between and among its users free of charge. The court stated that "[t]he ability to block infringers' access to a particular environment for any reason whatsoever is evidence of the right and ability to supervise." However, the court went on to explain that "[t]o escape imposition of vicarious liability, the reserved right to police must be exercised to its fullest extent. Turning a blind eye to *detectable* acts of infringement for the sake of profit gives rise to liability." (emphasis added). There, plaintiffs were successful in establishing a likelihood of success on the merits where Napster controlled access to its system, reserved the right to terminate user accounts for any reason and had the ability to locate infringing material listed on its search indices, but nonetheless failed to police its system to prevent the exchange of copyrighted material.

More recently in the electronic commerce context, other businesses have been found not to have the requisite right and ability to control infringing activity. For example, in *Amazon.com, Inc*., Google was found not to have the right and ability to control the infringing activity of third-party websites where Google did not have contractual relationships with the third-party websites and lacked the practical ability to police their activities. In *Visa Int'l Service Ass'n*, plaintiff alleged that Visa was secondarily liable for copyright infringement because its credit card payment services facilitated the purchase of infringing material online. Affirming the dismissal of those claims, the Ninth Circuit concluded that Visa lacked the ability to block access to the Internet or to particular websites and had no role in the alleged infringing activity. Although Visa could exert financial pressure by blocking access to its payment systems, the court concluded that "[f]or vicarious liability to attach ... the defendant must have the right and ability to *supervise and control* the infringement, not just affect it, and Defendants do not have this right or ability."

By contrast, an on-line age verification service was found to have the requisite "something more" than the mere ability to remove or block access to its website where it prescreened

websites within its network, gave those websites extensive advice, and prohibited the proliferation of identical sites within its network.

In the instant case, plaintiff maintains that Veoh has precisely the kind of control found in *Napster* and goes even further than the defendant in *Cybernet Ventures*. It points out that Veoh operates a closed system network requiring user registration, maintains a central index of video files on its servers, reserves the right to terminate user accounts for any reason, has the ability to remove infringing material from its website, and can even disable access to such material on its users' hard drives (assuming their computers are still connected to the Internet). It argues that the requisite control is further evidenced by the creation of the Flash and still-image files, the indexing of those files, Veoh's ability to feature certain videos on portions of its website, and by the fact that users are required to agree that Veoh shall have the irrevocable and perpetual right to distribute submitted material freely on its website.

However, Veoh is distinct from *Napster* in at least one significant respect. *Napster* existed solely to provide the site and facilities for copyright infringement, and its control over its system was directly intertwined with its ability to control infringing activity. See also Visa Int'l Service Ass'n, 494 F.3d at 799 n. 10 ("In fact, as virtually every interested college student knew—and as the program's creator expressly admitted—the *sole purpose* of the Napster program was to provide a forum for easy copyright infringement.").

Here, by contrast, Veoh's right and ability to control its system does not equate to the right and ability to control infringing activity. Unlike *Napster*, there is no suggestion that Veoh aims to encourage copyright infringement on its system. And, there is no evidence that Veoh can control what content users choose to upload before it is uploaded. Plaintiff suggests that Veoh should be required to prescreen every submission before it is published. However, Veoh has submitted evidence indicating that it has received hundreds of thousands of video files from users. Plaintiff has presented no evidence to refute those numbers; and, this court finds that no reasonable juror could conclude that a comprehensive review of every file would be feasible.

Even if such a review were feasible, there is no assurance that Veoh could have accurately identified the infringing content in question. True, Veoh maintains a central index of videos on its servers. However, unlike Napster (whose index was comprised entirely of pirated material), Veoh's ability to control its index does not equate to an ability to identify and terminate *infringing* videos. For the most part, the files in question did not bear titles resembling plaintiff's works; and, Io did not provide Veoh with its titles to search. The record suggests that, upon review of the files, Io itself was not able to readily identify which of its works allegedly were infringed. It initially alleged copyright violations as to eight films. However, in the course of discovery, it dropped one of those films and added three others.

Perhaps most importantly, there is no indication that Veoh has failed to police its system to the fullest extent permitted by its architecture. See Napster, 239 F.3d at 1024 (stating that the "reserved 'right and ability' to police is cabined by the system's current architecture."). Plaintiff has presented no evidence raising a genuine issue of material fact as to Veoh's enforcement of its terms of use, including through the termination of access to allegedly infringing material and the termination of user accounts for policy violations. As discussed above, the record presented

shows that Veoh has taken down blatantly infringing content, promptly responds to infringement notices, terminates infringing content on its system and its users' hard drives (and prevents that same content from being uploaded again), and terminates the accounts of repeat offenders. Once content has been identified as infringing, Veoh's digital fingerprint technology also prevents the same infringing content from ever being uploaded again. All of this indicates that Veoh has taken steps to reduce, not foster, the incidence of copyright infringement on its website.

Plaintiff nevertheless argues that Veoh should have changed its business operations to prevent infringing activity from occurring on its site. Specifically, it contends that Veoh should have verified the source of all incoming videos by obtaining and confirming the names and addresses of the submitting user, the producer, as well as the submitting user's authority to upload a given file. It further asserts that California Penal Code § 653w[11] and 18 U.S.C. § 2257 (the federal labeling law discussed above) require as much and that the allegedly infringing conduct in question should have been readily apparent in view of the requirements of those statutes. Alternatively, plaintiff contends that, if Veoh cannot prevent infringement on its site given the current volume of its business, then Veoh should be required to either hire more employees or to decrease its operations and limit its business to a manageable number of users (whatever that number might be). Its not-so-subtle suggestion is that, if Veoh cannot prevent infringement from ever occurring, then it should not be allowed to exist.

The issue here is not Veoh's compliance with California Penal Code § 653w and 18 U.S.C. § 2257. Nor is the issue whether Veoh should have been aware of that certain content was infringing. Rather the question is whether Veoh declined to exercise a right to stop it. Declining to change business operations is not the same as declining to exercise a right and ability to control infringing activity. Moreover, as discussed above, the DMCA does not require service providers to deal with infringers in a particular way. Here, there is no genuine issue of material fact that Veoh actively enforces its user policy and acts expeditiously to remove, or disable access to infringing material. Further, plaintiff's suggestion that Veoh must be required to reduce or limit its business operations is contrary to one of the stated goals of the DMCA. The DMCA was intended to facilitate the growth of electronic commerce, not squelch it. S.Rep. No. 105-190, at 1-2 (105th Congress, 2d Session 1998).

In sum, Io has not raised a genuine issue of material fact that Veoh had the right and ability to control the alleged infringing activity on veoh.com. This court finds that there is no triable fact issue as to whether Veoh qualifies for safe harbor under section 512(c) with respect to the alleged infringing activity in question.

While the DMCA's safe harbors do not immunize qualified service providers from liability, "[t]hey do ... protect eligible service providers from all monetary and most equitable relief that may arise from copyright liability." Because the court finds that, under the particular facts presented here, Veoh qualifies for safe harbor under Section 512(c), the only relief available to plaintiff is the limited injunctive relief under Section 512(j). In this case, before it ever received notice of any claimed infringement, Veoh independently removed all adult content, including video files of plaintiff's works, and it no longer allows such material on veoh.com. Thus, any

[11] Briefly stated, California Penal Code section 653w prohibits the knowing possession of a "physical embodiment" of an audiovisual work that does not identify the manufacturer and author.

injunctive relief to which Io would be entitled is moot. Because an opinion as to Veoh's liability for copyright infringement would be merely advisory, this court does not reach the issues raised in plaintiff's motion for summary judgment.

IV. CONCLUSION

The ever expanding realm of the Internet provides many new ways for people to connect with one another. This court appreciates that these new opportunities also present new challenges to the protection of copyright in the online world; and, the decision rendered here is confined to the particular combination of facts in this case and is not intended to push the bounds of the safe harbor so wide that less than scrupulous service providers may claim its protection. Nevertheless, the court does not find that the DMCA was intended to have Veoh shoulder the entire burden of policing third-party copyrights on its website (at the cost of losing its business if it cannot). Rather, the issue is whether Veoh takes appropriate steps to deal with copyright infringement that takes place. The record presented demonstrates that, far from encouraging copyright infringement, Veoh has a strong DMCA policy, takes active steps to limit incidents of infringement on its website and works diligently to keep unauthorized works off its website. In sum, Veoh has met its burden in establishing its entitlement to safe harbor for the alleged infringements here….

Viacom Intern. Inc. v. YouTube, Inc., 2010 WL 2532404 (S.D.N.Y. 2010).
Stanton, District Judge.

Defendants move for summary judgment that they are entitled to the Digital Millennium Copyright Act's ("DMCA"), 17 U.S.C. § 512(c), "safe harbor" protection against all of plaintiffs' direct and secondary infringement claims, including claims for "inducement" contributory liability, because they had insufficient notice, under the DMCA, of the particular infringements in suit.

Plaintiffs cross-move for partial summary judgment that defendants are not protected by the statutory "safe harbor" provision, but "are liable for the intentional infringement of thousands of Viacom's copyrighted works, ... for the vicarious infringement of those works, and for the direct infringement of those works ... because: (1) Defendants had 'actual knowledge' and were 'aware of facts and circumstances from which infringing activity [was] apparent,' but failed to 'act[ ] expeditiously' to stop it; (2) Defendants 'receive[d] a financial benefit directly attributable to the infringing activity' and 'had the right and ability to control such activity;' and (3) Defendants' infringement does not result solely from providing 'storage at the direction of a user' or any other Internet function specified in section 512."…

[the court then recapped the statute and its legislative history].

The tenor of the foregoing provisions is that the phrases "actual knowledge that the material or an activity" is infringing, and "facts or circumstances" indicating infringing activity, describe knowledge of specific and identifiable infringements of particular individual items. Mere knowledge of prevalence of such activity in general is not enough. That is consistent with an area of the law devoted to protection of distinctive individual works, not of libraries. To let knowledge of a generalized practice of infringement in the industry, or of a proclivity of users to post infringing materials, impose responsibility on service providers to discover which of their users' postings infringe a copyright would contravene the structure and operation of the DMCA. As stated in Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1113 (9th Cir. 2007):

> The DMCA notification procedures place the burden of policing copyright infringement-identifying the potentially infringing material and adequately documenting infringement-squarely on the owners of the copyright. We decline to shift a substantial burden from the copyright owner to the provider....

That makes sense, as the infringing works in suit may be a small fraction of millions of works posted by others on the service's platform, whose provider cannot by inspection determine whether the use has been licensed by the owner, or whether its posting is a "fair use" of the material, or even whether its copyright owner or licensee objects to its posting. The DMCA is explicit:

> it shall not be construed to condition "safe harbor" protection on "a service provider monitoring its service or affirmatively seeking facts indicating infringing activity...."

Indeed, the present case shows that the DMCA notification regime works efficiently: when Viacom over a period of months accumulated some 100,000 videos and then sent one mass take-down notice on February 2, 2007, by the next business day YouTube had removed virtually all of them.

2. Case Law

In *CCBill LLC*, supra, the defendants provided web hosting and other services to various websites. The plaintiff argued that defendants had received notice of apparent infringement from circumstances that raised "red flags": websites were named "illegal.net" and "stolencelebritypics.com," and others involved "password-hacking." As to each ground, the Ninth Circuit disagreed, stating "We do not place the burden of determining whether photographs are actually illegal on a service provider"; and "There is simply no way for a service provider to conclude that the passwords enabled infringement without trying the passwords, and verifying that they enabled illegal access to copyrighted material. We impose no such investigative duties on service providers."

The District Court in UMG Recordings, Inc. v. Veoh Networks, Inc., 665 F. Supp. 2d 1099, 1108 (C.D. Cal. 2009), concluded that "*CCBill* teaches that if investigation of 'facts and circumstances' is required to identify material as infringing, then those facts and circumstances are not 'red flags.' "That observation captures the reason why awareness of pervasive copyright-infringing, however flagrant and blatant, does not impose liability on the service provider. It furnishes at most a statistical estimate of the chance any particular posting is infringing—and that is not a "red flag" marking any particular work.

In Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1108 (W.D. Wash. 2004) the court stated that "The issue is not whether Amazon had a general awareness that a particular type of item may be easily infringed. The issue is whether Amazon actually knew that specific zShops vendors were selling items that infringed Corbis copyrights." It required a "showing that those sites contained the type of blatant infringing activity that would have sent up a red flag for Amazon." Other evidence of "red flags" was unavailing, for it "provides no evidence from which to infer that Amazon was aware of, but chose to ignore, red flags of blatant copyright infringement on specific zShops sites."

A similar recent decision of the Second Circuit involved analogous claims of trademark infringement (and therefore did not involve the DMCA) by sales of counterfeit Tiffany merchandise on eBay, Inc.'s website. In Tiffany (NJ) Inc. v. eBay Inc., 600 F.3d 93 (2d Cir. April 1, 2010) the Court of Appeals affirmed the dismissal of trademark infringement and dilution claims against eBay's advertising and listing practices. The sellers on eBay offered Tiffany sterling silver jewelry of which a significant portion (perhaps up to 75%) were counterfeit, although a substantial number of Tiffany goods sold on eBay were authentic. The particular issue was "whether eBay is liable for contributory trademark infringement—i.e., for culpably facilitating the infringing conduct of the counterfeiting vendors" because "eBay continued to supply its services to the sellers of counterfeit Tiffany goods while knowing or having reason to know that such sellers were infringing Tiffany's mark." Tiffany alleged that eBay knew, or had reason to know, that counterfeit Tiffany goods were being sold "ubiquitously" on eBay, and the District Court had found that eBay indeed "had *generalized*

notice that some portion of the Tiffany goods sold on its website might be counterfeit." Nevertheless, the District Court (Sullivan, J.) dismissed, holding that such generalized knowledge was insufficient to impose upon eBay an affirmative duty to remedy the problem. It held that "for Tiffany to establish eBay's contributory liability, Tiffany would have to show that eBay 'knew or had reason to know of specific instances of actual infringement' beyond those that it addressed upon learning of them."

The Court of Appeals held:

> We agree with the district court. For contributory trademark infringement liability to lie, a service provider must have more than a general knowledge or reason to know that its service is being used to sell counterfeit goods. Some contemporary knowledge of which particular listings are infringing or will infringe in the future is necessary.
>
> eBay appears to concede that it knew as a general matter that counterfeit Tiffany products were listed and sold through its website. Without more, however, this knowledge is insufficient to trigger liability under Inwood.

Although by a different technique, the DMCA applies the same principle, and its establishment of a safe harbor is clear and practical: if a service provider knows (from notice from the owner, or a "red flag") of specific instances of infringement, the provider must promptly remove the infringing material. If not, the burden is on the owner to identify the: infringement. General knowledge that infringement is "ubiquitous" does not impose a duty on the service provider to monitor or search its service for infringements.

3. The Grokster Case

Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005) and its progeny Arista Records LLC v. Usenet.com, Inc., 633 F. Supp. 2d 124 (S.D.N.Y. 2009) (dismissing DMCA defense as sanction for spoliation and evasive discovery tactics), Columbia Pictures Industries, Inc. v. Fung, 2009 U.S. Dist. LEXIS 122661 (C.D. Cal. Dec. 21, 2009), and Arista Records LLC v. Lime Group LLC, 2010 WL 2291485 (S.D.N.Y. May 25, 2010), which furnish core principles heavily relied on by plaintiffs and their supporting amici, have little application here. *Grokster*, *Fung*, and *Lime Group* involved peer-to-peer file-sharing networks which are not covered by the safe harbor provisions of DMCA § 512(c). The *Grokster* and *Lime Group* opinions do not even mention the DMCA. Fung was an admitted copyright thief whose DMCA defense under § 512(d) was denied on undisputed evidence of "'purposeful, culpable expression and conduct' aimed at promoting infringing uses of the websites."

Grokster addressed the more general law of contributory liability for copyright infringement, and its application to the particular subset of service providers protected by the DMCA is strained. In a setting of distribution of software products that allowed computer-to-computer exchanges of infringing material, with the expressed intent of succeeding to the business of the notoriously infringing Napster the *Grokster* Court held:

> ... that one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties.

On these cross-motions for summary judgment I make no findings of fact as between the parties, but I note that plaintiff Viacom's General Counsel said in a 2006 e-mail that "... the difference between YouTube's behavior and Grokster's is staggering." Defendants asserted in their brief supporting their motion and Viacom's response does not controvert that:

> It is not remotely the case that YouTube exists "solely to provide the site and facilities for copyright infringement." ... Even the plaintiffs do not (and could not) suggest as much. Indeed, they have repeatedly acknowledged the contrary.

The *Grokster* model does not comport with that of a service provider who furnishes a platform on which its users post and access all sorts of materials as they wish, while the provider is unaware of its content, but identifies an agent to receive complaints of infringement, and removes identified material when he learns it infringes. To such a provider, the DMCA gives a safe harbor, even if otherwise he would be held as a contributory infringer under the general law. In this case, it is uncontroverted that when YouTube was given the notices, it removed the material. It is thus protected "from liability for all monetary relief for direct, vicarious and contributory infringement" subject to the specific provisions of the DMCA.

4. Other Points

(a)

Plaintiffs claim that the replication, transmittal and display of videos on YouTube fall outside the protection § 512(c)(1) of the DMCA gives to "infringement of copyright by reason of the storage at the direction of a user of material" on a service provider's system or network. That confines the word "storage" too narrowly to meet the statute's purpose.

In § 512(k)(1)(B) a "service provider" is defined as "a provider of online services or network access, or the operator of facilities therefor," and includes "an entity offering the transmission, routing, or providing of connections for digital online communications." Surely the provision of such services, access, and operation of facilities are within the safe harbor when they flow from the material's placement on the provider's system or network: it is inconceivable that they are left exposed to be claimed as unprotected infringements. As the Senate Report states:

> In the ordinary course of their operations service providers must engage in all kinds of acts that expose them to potential copyright infringement liability.... In short, by limiting the liability of service providers, the DMCA ensures that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will continue to expand.

As stated in Io Group, Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132, 1148 (N.D. Cal. 2008), such "means of facilitating user access to material on its website" do not cost the service

provider its safe harbor. See also UMG Recordings, Inc. v. Veoh Networks, Inc., 620 F. Supp. 2d 1081, 1089 (C.D. Cal. 2008):

> Although Veoh correctly observes that the language of § 512(c) is "broad," it does not venture to define its outermost limits. It is unnecessary for this Court to do so either, because the critical statutory language really is pretty clear. Common sense and widespread usage establish that "by reason of" means "as a result of" or "something that can be attributed to...." So understood, when copyrighted content is displayed or distributed on Veoh it is "as a result of" or "attributable to" the fact that users uploaded the content to Veoh's servers to be accessed by other means. If providing access could trigger liability without the possibility of DMCA immunity, service providers would be greatly deterred from performing their basic, vital and salutary function-namely, providing access to information and material for the public.

To the extent defendants' activities go beyond what can fairly be characterized as meeting the above-described collateral scope of "storage" and allied functions, and present the elements of infringements under existing principles of copyright law, they are not facially protected by § 512(c). Such activities simply fall beyond the bounds of the safe harbor and liability for conducting them must be judged according to the general law of copyright infringement. That follows from the language of § 512(c)(1) that "A service provider shall not be liable ... for infringement of copyright by reason of the storage...." However, such instances have no bearing on the coverage of the safe harbor in all other respects.

(b)

The safe harbor requires that the service provider "not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity ..." The "right and ability to control" the activity requires knowledge of it, which must be item-specific. There may be arguments whether revenues from advertising, applied equally to space regardless of whether its contents are or are not infringing, are "directly attributable to" infringements, but in any event the provider must know of the particular case before he can control it. As shown by the discussion in Parts 1 and 2 above, the provider need not monitor or seek out facts indicating such activity. If "red flags" identify infringing material with sufficient particularity, it must be taken down.

(c)

Three minor arguments do not singly or cumulatively affect YouTube's safe harbor coverage.

(1) YouTube has implemented a policy of terminating a user after warnings from YouTube (stimulated by its receipt of DMCA notices) that the user has uploaded infringing matter (a "three strikes" repeat-infringer policy). That YouTube counts as only one strike against a user both (1) a single DMCA takedown notice identifying multiple videos uploaded by the user, and (2) multiple take-down notices identifying videos uploaded by the user received by YouTube within a two-hour period, does not mean that the policy was not "reasonably implemented" as required by § 512(i)(1)(A). In Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1105 (W.D. Wash. 2004), in evaluating whether Amazon complied with § 512(i), the Court stated that

even DMCA-compliant notices "did not, in themselves, provide evidence of blatant copyright infringement." In UMG Recordings, Inc. v. Veoh Networks, Inc., 665 F. Supp. 2d 1099, 1116, 1118 (C.D. Cal. 2009), the Court upheld Veoh's policy of terminating users after a second warning, even if the first warning resulted from a take-down notice listing multiple infringements. It stated:

> As the *Corbis* court noted, "[t]he key term, 'repeat infringer,' is not defined.... The fact that Congress chose not to adopt such specific provisions when defining a user policy indicates its intent to leave the policy requirements, and the subsequent obligations of the service providers, loosely defined." This Court finds that Veoh's policy satisfies Congress's intent that "those who repeatedly or flagrantly abuse their access to the Internet through disrespect for the intellectual property rights of others should know that there is a realistic threat of losing that access."

(2) In its "Claim Your Content" system, YouTube used Audible Magic, a fingerprinting tool which removed an offending video automatically if it matched some portion of a reference video submitted by a copyright owner who had designated this service. It also removed a video if the rights-holder operated a manual function after viewing the infringing video. YouTube assigned strikes only when the rights-holder manually requested the video to be removed. Requiring the rights-holder to take that position does not violate § 512(i)(1)(A). See UMG Recordings, 665 F. Supp. 2d at 1116-18 (automated Audible Magic filter "does not meet the standard of reliability and verifiability required by the Ninth Circuit in order to justify terminating a user's account"); see also Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1112 (9th Cir. 2007) ("We therefore do not require a service provider to start potentially invasive proceedings if the complainant is unwilling to state under penalty of perjury that he is an authorized representative of the copyright owner, and that he has a good-faith belief that the material is unlicensed.").

YouTube's initial hesitation in counting such rights-holder requests as strikes was reasonable: the six month delay was needed to monitor the system's use by rights-holders, and for engineering work to assure that strikes would be assigned accurately.

(3) Plaintiffs complain that YouTube removes only the specific clips identified in DMCA notices, and not other clips which infringe the same works. They point to the provision in § 512(c)(3)(A)(ii) that a notification must include "Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site." This "representative list" reference would eviscerate the required specificity of notice if it were construed to mean a merely generic description ("all works by Gershwin") without also giving the works' locations at the site, and would put the provider to the factual search forbidden by § 512(m). Although the statute states that the "works" may be described representatively, 512(c)(3)(A)(ii), the subsection which immediately follows requires that the identification of the infringing material that is to be removed must be accompanied by "information reasonably sufficient to permit the service provider to locate the material." 512(c)(3)(A)(iii). See House Report at 55; Senate Report at 46: "An example of such sufficient information would be a copy or description of the allegedly infringing material and the so-called "uniform resource locator" (URL) (i.e., web site address)

which allegedly contains the infringing material." See also UMG Recordings, 665 F. Supp. 2d at 1109-10 (DMCA notices which demanded removal of unspecified clips of video recordings by certain artists did not provide "'information reasonably sufficient to permit the service provider to locate [such] material.'") (alteration in original).

4.Conclusion

Defendants are granted summary judgement that they qualify for the protection of U.S.C. § 512(c), as expounded above, against all of plaintiff's claims for direct and secondary copyright infringement. Plaintiff's motion for judgement are denied….

Ticketmaster L.L.C. v. RMG Technologies, Inc., 507 F. Supp. 2d 1096 (C.D. Cal. 2007).
Collins, District Judge.

…I. FACTUAL AND PROCEDURAL BACKGROUND

In this action, Plaintiff Ticketmaster ("Plaintiff" or "Ticketmaster") alleges that Defendant RMG has developed and marketed automated devices to access and navigate through Ticketmaster's website, thereby infringing Plaintiff's copyrights and violating the website's Terms of Use and a number of federal and state statutes.

Plaintiff Ticketmaster sells tickets for entertainment and sports events on behalf of its clients to the general public through a variety of means, including its copyrighted website ticketmaster.com ("website"). Recognizing that competition to purchase tickets can be intense, Plaintiff contends that it attempts to ensure a fair and equitable ticket buying process on the website by contract and through technological means. First, visitors to ticketmaster.com are required to accept contractual provisions set forth in the website's "Terms of Use." These terms permit viewers to use ticketmaster.com for personal use only, prohibit commercial use, prohibit the use of automatic devices, prohibit users from accessing ticketing pages more than once during any three second interval, and prohibit consumers from purchasing more than a specific number of tickets in a single transaction.

Second, Plaintiff contends that it employs a number of technological means to ensure that ticket buying over the website is fair and equitable. One of these measures is a computer security program known as CAPTCHA that is designed to distinguish between human users and computer programs, and thereby prevent purchasers from using automated devices to purchase tickets.

Plaintiff contends that Defendant RMG has marketed and sold applications that enable Defendant's customers to use automated devices to enter and navigate through its website in violation of the Terms of Use governing the website, thereby causing injury to Plaintiff. For example, Plaintiff contends that Defendant's applications are prohibited "automatic devices," that the applications circumvent Plaintiff's access control and copy protection systems, including CAPTCHA, inundate Plaintiff's computers with thousands of automatic requests thereby preventing ordinary consumers from accessing the website, and enable Defendant's clients to purchase large quantities of tickets. Based on these allegations, Plaintiff's FAC, filed on June 25, 2007, states eleven causes of action against Defendant.

Plaintiff now moves for a preliminary injunction based on five of its claims. Plaintiff's evidence in support of its motion includes declarations from its Senior Director of Applications Support, Kevin McLain, wherein Mr. McLain testifies how he was able to trace ticket requests and purchases made on ticketmaster.com back to individual users and, ultimately, to Defendant. Based on his methodology, McLain discovered, for example, that Chris Kovach, a ticket broker and one of Defendant's clients, purchased over 9,500 ticket orders—or 24,000 tickets—over the last several years. McLain also explains that he identified Gary Charles Bonner and Thomas J. Prior as Defendant's clients. Using IP addresses registered to Defendant, Bonner made almost 13,000 ticket purchases over several years, and made more than 425,000 ticket requests in a

single day. Using IP addresses registered to Defendant, Prior made almost 22,000 ticket orders over several years, and made more than 600,000 ticket requests in a single day. Plaintiff also submitted declarations from Kovach; Adam Lieb, a computer and internet consultant; Steven Obara, Plaintiff's Director of Customer Service Operations; Mark Lee, an attorney representing Plaintiff in this matter; and a number of exhibits.

Defendant challenges the Motion on both legal and factual grounds. Defendant states that the computer application Plaintiff seeks to enjoin Defendant from using and selling is its Ticket Broker Acquisition Tool ("TBAT"), and that this application is not an "automated device" but, rather, is simply a type of internet browser, akin to Internet Explorer, requiring human interaction. Defendant also urges that it should not be bound by the Terms of Use and that, in any case, Plaintiff has presented no evidence upon which it—as opposed to the persons using TBAT—can be enjoined. Defendant also argues that Plaintiff's legal theories are flawed in various ways….

III. ANALYSIS

The five claims on which Plaintiff seeks a preliminary injunction are its claims for violation of the United States Copyright Act, 17 U.S.C. §§ 501 et seq., the Digital Millennium Copyright Act ("DMCA") 17 U.S.C. § 1201, California Penal Code § 502, and the Computer Fraud and Abuse Act ("CFAA") 18 U.S.C. § 1030(g), and on its breach of contract claim.

A. Likelihood of Success on the Merits.

1. Plaintiff's Copyright Claim

To prevail on its claim for copyright infringement, Plaintiff must (1) "show ownership of the allegedly infringed material and (2) [it] must demonstrate that the alleged infringers violate at least one exclusive right granted to copyright holders under 17 U.S.C. § 106." Ticketmaster alleges that RMG is violating its copyright in the ticketmaster.com website.

Ticketmaster has submitted evidence that it owns registered copyrights in the website ticketmaster.com, and, separately, in portions of the website. "A website may constitute a work of authorship fixed in a tangible medium of expression ... Copyright protection for a website may extend to both the screen displays and the computer code for the website." Defendant does not dispute Plaintiff's claim that its website is copyrighted. Ticketmaster has thus satisfied the first element of its copyright claim.

Ticketmaster alleges that RMG infringes its copyrights in ticketmaster.com both directly and indirectly. First, Ticketmaster states that each time Defendant views a page from ticketmaster.com, a copy of that page is necessarily downloaded or "cached" from Plaintiff's computers onto the Defendant's computer's random access memory ("RAM"), thus rendering Defendant *directly liable* for such copying. Plaintiff also argues that Defendant directly participates in its customers' unauthorized access of the website because its customers do not acquire physical possession of the software. Rather, Defendant's devices are kept on Defendant's own computer systems; in order to gain access to Defendant's devices, its customers must log onto Defendant's website ticketbrokertools.com, and use the devices hosted on

ticketbrokertools.com to improperly access ticketmaster.com. Thus, Defendant allows and, indeed, requires its customers to go through its own infrastructure in order to employ the devices that access ticketmaster.com. Defendant denies this factual allegation and states that "TBAT [has never been] operated from RMG's computer system on behalf of any client, as it is not, nor has it ever, been centrally run on behalf of any client."

Second, Plaintiff states that Defendant is *indirectly liable* for contributory infringement, vicarious infringement, and inducing copyright infringement because it provides its clients with bots and other automated devices to infringe Plaintiff's copyright in its website. Both direct and indirect infringement occur insofar as the person viewing the website does so in excess of the authorization Plaintiff grants through the website's Terms of Use.

a. Defendant's Direct Liability for Copyright Infringement
Defendant's direct liability for copyright infringement is based on the automatically-created copies of ticketmaster.com webpages that are stored on Defendant's computer each time Defendant accesses ticketmaster.com. Defendant does not contest that, as a technological question, whenever a webpage is viewed on a computer, copies of the viewed pages are made and stored on the viewer's computer. However, Defendant contends that such "cached" copies are not "copies" within the meaning of the Copyright Act, that such copies could not give rise to copyright liability because their creation constitutes fair use, and that Plaintiff has not shown that any pages from ticketmaster.com were ever downloaded or stored on Defendant's computer.

Section 101 of the Copyright Act defines "copies" as "material objects, other than phonorecords, in which a work is fixed by any method now known or later developed, and from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device." The Copyright Act also provides that "[a] work is 'fixed' in a tangible medium of expression when its embodiment in a copy or phonorecord, by or under the authority of the author, is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration."

The copies of webpages stored automatically in a computer's cache or random access memory ("RAM") upon a viewing of the webpage fall within the Copyright Act's definition of "copy." See, e.g., MAI Systems Corp. v. Peak Computer, Inc., 991 F.2d 511, 519 (9th Cir. 1993) ("We recognize that these authorities are somewhat troubling since they do not specify that a copy is created regardless of whether the software is loaded into the RAM, the hard disk or the read only memory ('ROM'). However, since we find that the copy created in the RAM can be 'perceived, reproduced, or otherwise communicated,' we hold that the loading of software into the RAM creates a copy under the Copyright Act.") See also Twentieth Century Fox Film Corp. v. Cablevision Systems Corp., 478 F. Supp. 2d 607, 621 (S.D.N.Y. 2007) (agreeing with the "numerous courts [that] have held that the transmission of information through a computer's random access memory or RAM ... creates a 'copy' for purposes of the Copyright Act," and citing cases.) Thus, copies of ticketmaster.com webpages automatically stored on a viewer's computer are "copies" within the meaning of the Copyright Act.

The Court must next determine whether Plaintiff has shown by a preponderance of the evidence that Defendant did in fact view the website, thereby copying its webpages. Although Plaintiff

does not present direct evidence of such viewing, the logic from which such an inference may be drawn is compelling. Plaintiff presents expert testimony that Defendant necessarily had to view ticketmaster.com in order to create the applications that enable Defendant's customers to enter and navigate through the website. Indeed, in order to test the applications to determine whether they worked as intended, Defendant would have had to actually use the applications to purchase tickets from the website. By Defendant's own description, TBAT is "a browser geared for the purchase of tickets from a variety of websites including ... ticketmaster.com." It also follows that Defendant's clients would have had to visit the website, and thus copy pages, in order to make ticket purchases. The Court thus finds that Plaintiff is indeed likely to prove that Defendant visited (and used) ticketmaster.com and necessarily made copies of pages from the copyrighted website.

Plaintiff also argues that Defendant is directly liable for infringement because its clients must work through Defendant's website and computer system in order to use Defendant's ticket purchasing software and thereby gain unauthorized access to ticketmaster.com. Defendant disputes this allegation. However, the Court finds it unnecessary to decide whether Plaintiff will prevail in its claim for direct infringement by showing that Defendant directly participates in its clients' conduct by acting as an intermediary for their unauthorized use of ticketmaster.com. As discussed above, Plaintiff will likely succeed in its claim for direct liability by showing that Defendant itself viewed and/or used the website.[4]

Next, the Court will consider whether Plaintiff is likely to demonstrate that such copying constitutes copyright infringement. Plaintiff contends that Defendant infringed its copyrights by accessing and using the copyrighted website in excess of the authorization granted in the website's Terms of Use, which Plaintiff contends creates a non-exclusive license to view (and thus copy) pages from the website. Defendant presents a number of legal and factual arguments against this theory, but none of them is meritorious.

First, the Court agrees that the Terms of Use presented on ticketmaster.com create a non-exclusive license to copy the website. "The word 'license,' means permission, or authority; and a license to do any particular thing, is a permission or authority to do that thing." "No magic words must be included in a document" to create a copyright license. Radio Television Espanola S.A. v. Furthermore, nonexclusive licenses can be implied from conduct. See Effects Associates, Inc. v. Cohen, 908 F.2d 555, 558-559 (9th Cir. 1990) (holding that by creating a work at defendant's request and handing it over to defendant to copy and distribute, plaintiff granted defendant an implied nonexclusive license to the work.) Use of a work in excess of a license gives rise to liability for copyright infringement.

Plaintiff has presented evidence showing that access to the website is governed by specific Terms of Use, and that any person viewing the website is put on notice of the Terms of Use. For example, the ticketmaster.com homepage displays the following warning: "Use of this website is subject to express Terms of Use which prohibit commercial use of this site. By continuing past this page, you agree to abide by these terms." The underlined phrase "Terms of Use" is a

[4] In addition, even accepting Defendant's version of the facts-that its clients download TBAT onto their own computers and operate it independent of Defendant-its conduct would still render it liable for contributory infringement, discussed infra.

hyperlink to the full Terms of Use; the same phrase appears on almost every page of ticketmaster.com. In addition, since 2003, users of ticketmaster.com have had to affirmatively agree to the Terms of Use as part of the procedure to set up an account, and since mid-2006, users have had to affirmatively agree to the Terms of Use for every ticket purchase.

Having determined that Plaintiff is highly likely to succeed in showing that Defendants viewed and navigated through ticketmaster.com, the Court further concludes that Plaintiff is highly likely to succeed in showing that Defendant received notice of the Terms of Use and assented to them by actually using the website. See, e.g., Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 248 (S.D.N.Y. 2000) (where website's terms of use stated "by submitting this query, you agree to abide by these terms," court held "there can be no question that [the user of website] manifested its assent to be bound" by the terms of use when it electronically submitted queries to the database); Hotmail Corp. v. Van$ Money Pie Inc., 1998 WL 388389, *2, 6 (N.D. Cal. 1998) (granting preliminary injunction based in part on breach of "Terms of Service" agreement, to which defendants had assented.) Indeed, Defendant does not contest that it was on notice of the Terms of Use; rather, Defendant argues that the Terms of Use do not amount to an agreement or a license, and that the Terms are too uncertain to be enforced. The Court finds no merit in these arguments.

The Terms of Use governing ticketmaster.com include the following terms:

> "You [the viewer] agree that you are only authorized to visit, view and to retain a copy of pages of this site for your own personal use, and that you shall not duplicate, download, [or] modify ... the material on this Site for any purpose other than to review event and promotions information, for personal use ..."
>
> "No ... areas of this Site may be used by our visitors for any commercial purposes ..."
>
> "You agree that you will not use any robot, spider or other automated device, process, or means to access the Site.... You agree that you will not use any device, software or routine that interferes with the proper working of the Site nor shall you attempt to interfere with the proper working of the Site."
>
> "You agree that you will not take any action that imposes an unreasonable or disproportionately large load on our infrastructure."
>
> "You agree that you will not access, reload or 'refresh' transactional event or ticketing pages, or make any other request to transactional servers, more than once during any three second interval."
>
> "You do not have permission to access this Site in any way that violates ... these terms of use."
>
> "You understand and agree that ... Ticketmaster may terminate your access to this Site, cancel your ticket order or tickets acquired through your ticket order ... if

> Ticketmaster believes that your conduct or the conduct of any person with whom Ticketmaster believes you act in concert ... violates or is inconsistent with these Terms or the law, or violates the rights of Ticketmaster, a client of Ticketmaster or another user of the Site."

Viewers are thus authorized to view—and thereby copy—pages of the website when they do so in accordance with the Terms of Use. In addition, Plaintiff reserves the right to terminate any person's access to the website if it believes that person violated the Terms of Use. Thus, by the Terms of Use, Plaintiff grants a nonexclusive license to consumers to copy pages from the website in compliance with those Terms. Inasmuch as Defendant used the website, Defendant assented to the terms.

Nor are the terms so vague as to be unenforceable. The above terms permit access for personal use only, prohibit commercial use, prohibit the use of bots and automated devices, limit the frequency with which users can make requests of the website, and require the user to agree not to interfere with the proper working of the website. Defendant argues, however, that the term "automated device" is confusing. Specifically, Defendant's President, Cipriano Garibay, a software designer, testifies in his declaration that TBAT—which he appears to claim is the only product in issue in this case—is just a web browser and is not an "automated device" because it requires human interaction to function. Garibay further claims that he does not know what Plaintiff is referring to by the term "automated device" because "every computer in the world, as well as all computer programs and web browsers, have [sic] a large degree of automation built in since they are not run manually. Clearly, Ticketmaster is not seeking to prohibit all computers and browsers from accessing its website, otherwise the website would be useless. However, as Ticketmaster has not defined 'automated device' in its 'Terms of Use,' I can only speculate as to what it means by same."

This claim is specious. First, the term appears in the provision in which website viewers agree to "not use any robot, spider or *other* automated device, process, or means to access the Site." (emphasis added). Although the terms of use include no additional definition of "automated device," they identify robots and spiders as examples of such devices, which Garibay states are "programs which by their very nature run without interfacing with humans." Plaintiff has submitted credible testimony showing that Defendant's applications are, in fact, automated devices. For example, Adam Lieb, a computer consultant who studied a directory Defendant placed on Kovach's computer, testified that "the term 'automated device' is easy to understand in the context of computer programming"—a field in which Garibay claims 10 years of experience—and that TBAT is an automated device. Lieb explains that even though TBAT may require human initialization or set up, the application generates automated requests thereafter. Based on his examination of the "super proxy" log files on Kovach's computer, Lieb states that "several webpage requests per second were made to Ticketmaster, via the proxy, from the same source IP address. Thousands of requests were made per day. No human would be able to generate that many requests during manual, non-automated web browsing. These were automated request[s] made by an 'automated device.'"

Based on his personal experience, Kovach describes Defendant's software as "including automated devices that RMG calls 'workers' that can automatically navigate the Ticketmaster

website.... [M]y level of service enabled me to use multiple workers—sometimes over one hundred of them—simultaneously to search for and request tickets." Kovach further describes how he could command the workers to search for tickets according to parameters that he would set, and that the workers would search for tickets automatically and alert him when they found tickets matching his parameters. Indeed, Defendant's own website advertises its products as "let[ting] you do the work of a dozen people at once. Just enter the event information ... and the moment the event goes on sale, PurchaseMaster goes into action." In view of all of the evidence, Plaintiff is highly likely to succeed on its claim that Defendant's applications are automated devices that violate the Terms of Use.

However, even setting aside Plaintiff's prohibition of automated devices, the application as described would violate other provisions of the Terms of Use. For example, using an application that enables a person to make several requests per second would violate the provision limiting the frequency of requests to no more than one every three seconds. Furthermore, use of an application designed to thwart Plaintiff's access control by, in Defendant's own description, "stealth technology [that] lets you hide your IP address, so you **never get blocked by Ticketmaster**," (original emphasis) would breach the user's agreement to "not use any device, software or routine that interferes with the proper working of the Site nor shall you attempt to interfere with the proper working of the Site." See also Kovach Decl. ¶ 8 (explaining his understanding that the "workers are specifically designed to navigate or otherwise avoid various security measures on Ticketmaster's website.")

Finally, Defendant argues in summary fashion that to the extent Plaintiff's claim is predicated on automatically-made cache copies of Plaintiff's webpages, such cache copies constitute fair use as a matter of law under Perfect 10, Inc., v. Amazon.com, Inc., 487 F.3d 701, 716 (9th Cir. 2007). This argument is unavailing for several reasons. First, "[b]ecause the defendant in an infringement action has the burden of proving fair use, the defendant is responsible for introducing evidence of fair use in responding to a motion for preliminary relief." Here, Defendant has come forward with no evidence of fair use. Nor did Defendant attempt to explain how its use satisfies any of the four fair use factors set forth in 17 U.S.C. § 107. Accordingly, the fair use defense fails to defeat Plaintiff's motion on these grounds alone.

Second, Perfect 10 does not stand for the absolute principle of law that Defendant attributes to it. Rather, Perfect 10 addressed, among other questions, whether users who link to infringing websites and thus make automatic cache copies of those infringing websites themselves commit copyright infringement. The Ninth Circuit agreed with the district court that such conduct was "fair use **in this context**" because the caching was "noncommercial, transformative ... and has a minimal impact on the potential market for the original work." Significantly, the Court also noted that "a cache copies no more than necessary to assist the user in Internet use," and, in the case before it, the "background copying has no more than a minimal effect" on the plaintiff's rights. In this context, by contrast, Defendant is not an "innocent" third-party visitor to another person's infringing site. Instead, the purpose of Defendant's viewing ticketmaster.com and the copying that necessarily entails is to engage in conduct that violates the Terms of Use in the ways described above. In addition, Defendant's use of the website is to further its own commercial objectives, that is, to create and sell ticket purchasing applications that can gain unauthorized access to ticketmaster.com. In addition, in this case, such copying has a significant,

as opposed to minimal, effect on Plaintiff's rights because Defendant's conduct empowers its customers to also violate the Terms of Use, infringe on Plaintiff's rights, and collectively cause Plaintiff the harm described below. For all of these reasons, Defendant's fair use defense fails.

Because the Court finds that Plaintiff has a strong likelihood of proving that Defendant violated ticketmaster.com' s Terms of Use by using automated devices, making excessive requests, and interfering with the proper working of the website when it used and/or designed applications that access ticketmaster.com, the Court finds that Plaintiff has a strong likelihood of succeeding on the merits of its claim for direct copyright infringement.

b. Defendant's Indirect Liability for Copyright Infringement
Plaintiff also argues that it has a strong likelihood of success on its claim for indirect copyright infringement. The Court agrees.

"One infringes contributorily by intentionally inducing or encouraging direct infringement, and infringes vicariously by profiting from direct infringement while declining to exercise a right to stop or limit it." Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 930-931 (2005). Although "[t]he Copyright Act does not expressly render anyone liable for infringement committed by another, these doctrines of secondary liability emerged from common law principles and are well established in the law." In *Grokster*, the Supreme Court held that "one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties." Evidence to support an inducement theory includes, for example "advertisement[s] or solicitation[s] that broadcast [ ] a message designed to stimulate others to commit violations." Here, as described above, there is substantial evidence that Defendant designed its application for the purpose of giving its clients unauthorized access to ticketmaster.com; Defendant even advertises its product as "stealth technology [that] lets you hide your IP address, so you **never get blocked by Ticketmaster**" (original emphasis.) Designing and marketing a device whose purpose is to allow unauthorized access to, and thus to infringe on, a copyrighted website is sufficient to trigger contributory liability for infringement committed by the device's immediate users. See, e.g., Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 264 (9th Cir. 1996) (stating that providing the site and facilities for known infringing activity is sufficient to establish contributory liability, and quoting with approval 2 William F. Patry, Copyright Law & Practice 1147, "Merely providing the means for infringement may be sufficient" to incur contributory copyright liability.)

As discussed in the Background section, Plaintiff has presented examples of Defendant's clients making numerous ticket purchases and ticket requests using Defendant's applications and resources, including the examples of Bonner making more than 425,000 requests in a single day, and Prior making more than 600,000 requests in a single day, both through IP addresses registered to Defendant. Requests so numerous cannot be made other than with automated devices. Kovach testified how he used Defendant's applications to make automated ticket requests, and that Defendant made representatives available to help him use its applications, circumvent Plaintiff's security measures, and set up his hardware for optimal use. Such uses infringe on Plaintiff's copyrights for the reasons stated above with regard to Defendant's direct infringement.

Based on this evidence, the Court finds that Plaintiff is highly likely to prove that Defendant induced or encouraged its clients' direct infringement by providing them with devices that gain them unauthorized access to and use of ticketmaster.com. Plaintiff is therefore highly likely to succeed in its claim against Defendant for contributory infringement.

2. Plaintiff's Claim Under the Digital Millennium Copyright Act

Plaintiff alleges that Defendant has violated the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 1201 et seq., by trafficking in technological products, services, devices, or components that are primarily designed to circumvent Plaintiff's access control and copy protection systems. Plaintiff's Motion relies on two provisions of the DMCA.

First, Plaintiff claims Defendant is liable under section 1201(a)(2), which prohibits trafficking in devices designed to circumvent "technological measure[s] that effectively control[ ] access to a work protected under this title." "A plaintiff alleging a violation of § 1201(a)(2) must prove: (1) ownership of a valid copyright on a work, (2) effectively controlled by a technological measure, which has been circumvented, (3) that third parties can now access (4) without authorization, in a manner that (5) infringes or facilitates infringing a right protected by the Copyright Act, because of a product that (6) the defendant either (i) designed or produced primarily for circumvention; (ii) made available despite only limited commercial significance other than circumvention; or (iii) marketed for use in circumvention of the controlling technological measure."

The Court finds that Plaintiff is likely to prevail on its section 1201(a)(2) claim. Specifically, as stated above, Plaintiff is likely to prove that (1) Plaintiff owns copyrights to ticketmaster.com and specific portions thereof; (2) Plaintiff employs "technological measures" such as CAPTCHA to block automated access to its copyrighted ticket purchase pages; (3) Defendant's customers are third parties who can now access those copyrighted pages; (4) these parties access those pages without Plaintiff's authorization; and (5) that this access infringes Plaintiff's rights because it entails copying those pages in excess of the third parties' license to do so; and (6)(i), (iii) these third parties have such access because of Defendant's products designed primarily for circumvention, and marketed for use in circumvention of the controlling technological measure.

The majority of Defendant's challenges to Plaintiff's Motion on the DMCA claim are repetitive of its arguments with regard to the copyright claim, and are unavailing for the same reasons. The only unique arguments as to the DMCA claim are that CAPTCHA is not a system or a program, but is simply an image, and that CAPTCHA is designed to regulate ticket sales, not to regulate access to a copyrighted work.

First, the Court notes that the DMCA does not equate its use of the term "technological measure" with Defendant's terms "system" or "program." In any case, Plaintiff has submitted evidence that CAPTCHA is a technological measure that regulates access to a copyrighted work. Although the DMCA does not appear to include a definition of the term, it states that "a technological measure 'effectively controls access to a work' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work." When the user makes a ticket request on ticketmaster.com, CAPTCHA presents "a box with stylized random characters partially obscured

behind hash marks." The user is required to type the characters into an entry on the screen in order to proceed with the request. Most automated devices cannot decipher and type the random characters and thus cannot proceed to the copyrighted ticket purchase pages. Thus, because CAPTCHA "in the ordinary course of its operation, requires the application of information ... to gain access to the work," it is a technological measure that regulates access to a copyrighted work. Plaintiff is therefore likely to prevail on its DMCA § 1201(a)(2) claim.

Section 1201(b)(1) similarly prohibits the trafficking of devices primarily designed or produced for the purpose of circumventing "protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof." Sections 1201(a)(2) and 1201(b)(1) differ only in that 1201(a)(2), by its terms, makes it wrongful to traffic in devices that circumvent technological measures that *control access to protected works*, while 1201(b)(1) makes it wrongful to traffic in devices that circumvent technological measures that *protect rights of a copyright owner in a work*. Here, CAPTCHA both *controls access* to a protected work because a user cannot proceed to copyright protected webpages without solving CAPTCHA, and *protects rights* of a copyright owner because, by preventing automated access to the ticket purchase webpage, CAPTCHA prevents users from copying those pages. For the foregoing reasons, the Court finds that Plaintiff is likely to prevail on its DMCA §§ 1201(a)(2) and 1201(b)(1) claims.

3. Plaintiff's Breach of Contract Claim

Plaintiff argues that Defendant is breaching the ticketmaster.com Terms of Use in numerous ways, and is therefore liable for breach of contract. The facts and issues that this claim raises are the same as those raised by Plaintiff's contention, in connection with its copyright claims, that Defendant breached the Terms of Use. The Court addressed the merits of that claim in its discussion of Plaintiff's claim for copyright infringement, and concluded that Plaintiff is highly likely to prove that use of ticketmaster.com is governed by the Terms of Use; that Defendant was on notice of, and assented to, the Terms of Use; and that Defendant violated the Terms of Use by using automated devices to access the website, using an application that makes several requests per second (in violation of the provision limiting the frequency of requests to no more than one every three seconds), and by using an application designed to thwart Plaintiff's access controls (which breaches the user's agreement to "not use any device, software or routine that interferes with the proper working of the Site nor shall you attempt to interfere with the proper working of the Site."). The Court therefore finds that Plaintiff is therefore likely to prevail on its breach of contract claim.

4. Plaintiff's Computer Fraud and Abuse Act Claim

Plaintiff also argues that it is likely to prevail on its claim under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. Although the CFAA is a criminal statute, it permits "any person who suffers damage or loss" through a violation of its provisions "to maintain a civil action ... to obtain compensatory damages and injunctive relief or other equitable relief." To prevail on its CFAA claim, Plaintiff must demonstrate that Defendant "intentionally accesse[d] a computer without authorization or exceed[ed] authorized access, and thereby obtain[ed] information from any protected computer," or that Defendant "knowingly cause[d] the transmission of a program ... and ... cause [d] damage without authorization to a protected

computer." Plaintiff must also demonstrate that Defendant's unauthorized access caused $5,000 in loss or damage during a one year period.

It appears likely that Plaintiff will be able to prove that Defendant gained unauthorized access to, and/or exceeded authorized access to, Plaintiff's protected computers, and caused damage thereby. Based on the statute and the cases Plaintiff cites, the Court also agrees that the required $5,000 of harm may consist of harm to a computer system, and need not be suffered by just one computer during one particular intrusion. However, because Plaintiff has not quantified its harm as required by the statute or even attempted to show what portion of the harm is attributable to Defendant, the Court cannot find that Plaintiff has affirmatively shown that its harm caused by Defendant exceeds the $5,000 minimum. Thus, the CFAA claim does not provide a basis for a preliminary injunction.

In light of the Court's rulings on Plaintiff's copyright, DMCA, and breach of contract claims, the Court need not address whether Plaintiff is likely to succeed on its claims under California Penal Code § 502, the fifth basis asserted for the preliminary injunction.

B. Irreparable Harm

Having determined that Plaintiff has a strong likelihood of success on the merits of its copyright, DMCA, and breach of contract claims, the Court now addresses whether Plaintiff has shown "the possibility of irreparable injury."

For Plaintiff's copyright claim, "a showing of a reasonable likelihood of success on the merits raises a presumption of irreparable harm." "A copyright holder seeking a preliminary injunction is therefore not required to make an independent demonstration of irreparable harm." Here, because Plaintiff has shown a strong likelihood of success on the merits of its copyright claim, the Court presumes irreparable harm. Defendant has done nothing to rebut that presumption.

The Court also finds that Plaintiff has otherwise shown the possibility of irreparable harm required to support the issuance of a preliminary injunction on its DMCA and breach of contract claims. Specifically, Plaintiff has submitted extensive evidence demonstrating that it is suffering a loss of goodwill with the buying public in that there is a growing public perception that Plaintiff does not provide the public with a fair opportunity to buy tickets due to automated purchases. Such evidence includes numerous complaints from consumers about the unavailability of tickets, some of which demonstrate extreme dissatisfaction with Plaintiff and indicate suspicions that Plaintiff is colluding with ticket brokers to deny consumers tickets.[5] Plaintiff has also submitted copies of consumer comments posted on blogs expressing similar extreme dissatisfaction[6] and evidence of numerous news stories discussing the unavailability of

[5] Plaintiff's brief quotes several of the complaints compiled in Exhibit 19. One such complaint states: "I would like to know how within 20 seconds of a show going on sale I could not find ANY seats together at ANY price at this event. However, there are gobs of them for sale on many different scalper sites. How is this possible and why is this tolerated. The only explanation for this is that people inside TM are in cahoots with these criminals. I would just like to know if there are any plans whatsoever to address this situation."

[6] For example, the following is a comment posted by someone who could not obtain tickets to a performance of the rock group "Rush": "I am absolutely irate about TicketBxxxxxd and its practices. As has been mentioned on this site

tickets. For example, many of the news stories concern the unavailability of tickets to concerts in Hannah Montana's "Best of Both Worlds" tour. Based on the reports, many parents expressed disappointed and outrage at Plaintiff because tickets to many Hannah Montana concerts throughout the nation (Bossier City, Louisiana; Miami, Florida; Atlanta, Georgia; and Kansas City, Missouri, for example) were snapped up within several hours—and sometimes within minutes—of their release for sale. It also appears that the public's difficulty obtaining tickets to the Hannah Montana concerts was so severe and created such an outcry that the Attorneys General of Missouri and Arkansas initiated investigations into Plaintiff's ticket selling practices….

Although the extent of Defendant's culpability for this harm to Plaintiff's goodwill cannot yet be determined, it is likely that some of Defendant's customers were able to obtain tickets to such concerts by using Defendant's applications. Given the alleged extent of Defendant's participation in the hundreds of thousands of automated ticket requests wrongfully made of Plaintiff's website, it is likely that Defendant's conduct has caused, and will continue to cause, some portion of Plaintiff's loss of goodwill unless Defendant's conduct is enjoined. As a consequence of Plaintiff's loss of consumer goodwill, Plaintiff also faces the possibility of loss of goodwill and loss of business from its clients.

In this Circuit, intangible injuries, such as damage to goodwill, can constitute irreparable harm. Plaintiff has also submitted evidence that it has attempted to use technological countermeasures to prevent automated ticket requests, but that these efforts have had only limited success. Thus, the Court is not persuaded by Defendant's argument that Plaintiff's self-help measures (such as "blacklisting" IP addresses) are enough to prevent irreparable harm and thus obviate the need for injunctive relief. In addition, the cost to Plaintiff of developing and implementing such countermeasures is not easily calculable. For the foregoing reasons, the Court finds that Plaintiff has demonstrated the possibility of irreparable harm….

---

already, the whole process of getting tickets to concerts has gotten completely out of control with scalpers, brokers, and God-knows-who-else trying to make a buck at the expense of fans."

Trademark FAQs Excerpts (from http://www.uspto.gov/web/offices/tac/tmfaq.htm) (accessed August 5, 2007) (omitted questions aren't indicated)

What is a trademark?
A trademark includes any word, name, symbol, or device, or any combination, used, or intended to be used, in commerce to identify and distinguish the goods of one manufacturer or seller from goods manufactured or sold by others, and to indicate the source of the goods. In short, a trademark is a brand name.

What is a service mark?
A service mark is any word, name, symbol, device, or any combination, used, or intended to be used, in commerce, to identify and distinguish the services of one provider from services provided by others, and to indicate the source of the services.

What is a certification mark?
A certification mark is any word, name, symbol, device, or any combination, used, or intended to be used, in commerce with the owner's permission by someone other than its owner, to certify regional or other geographic origin, material, mode of manufacture, quality, accuracy, or other characteristics of someone's goods or services, or that the work or labor on the goods or services was performed by members of a union or other organization.

What is a collective mark?
A collective mark is a trademark or service mark used, or intended to be used, in commerce, by the members of a cooperative, an association, or other collective group or organization, including a mark which indicates membership in a union, an association, or other organization.

Do I have to register my trademark?
No, but federal registration has several advantages, including notice to the public of the registrant's claim of ownership of the mark, a legal presumption of ownership nationwide, and the exclusive right to use the mark on or in connection with the goods or services set forth in the registration.

What are the benefits of federal trademark registration?
1. Constructive notice nationwide of the trademark owner's claim.
2. Evidence of ownership of the trademark.
3. Jurisdiction of federal courts may be invoked.
4. Registration can be used as a basis for obtaining registration in foreign countries.
5. Registration may be filed with U.S. Customs Service to prevent importation of infringing foreign goods.

Are there federal regulations governing the use of the designations "TM" or "SM" with trademarks?
No. Use of the symbols "TM" or "SM" (for trademark and service mark, respectively) may, however, be governed by local, state, or foreign laws and the laws of the pertinent jurisdiction must be consulted. These designations usually indicate that a party claims rights in the mark and are often used before a federal registration is issued.

When is it proper to use the federal registration symbol (the letter R enclosed within a circle — ® — with the mark.

The federal registration symbol may be used once the mark is actually registered in the U.S. Patent and Trademark Office. Even though an application is pending, the registration symbol may not be used before the mark has actually become registered. The federal registration symbol should only be used on goods or services that are the subject of the federal trademark registration. [Note: Several foreign countries use the letter R enclosed within a circle to indicate that a mark is registered in that country. Use of the symbol by the holder of a foreign registration may be proper.]

What constitutes interstate commerce?
For goods, "Interstate commerce" involves sending the goods across state lines with the mark displayed on the goods or the packaging for the goods. With services, "interstate commerce" involves offering a service to those in another state or rendering a service which affects interstate commerce (e.g. restaurants, gas stations, hotels, etc.).

Is a federal registration valid outside the United States?
No. However, if you are a qualified owner of a trademark application pending before the USPTO, or of a registration issued by the USPTO, you may seek registration in any of the countries that have joined the Madrid Protocol by filing a single application, called an "international application," with the he International Bureau of the World Property Intellectual Organization, through the USPTO. For more information about the Madrid Protocol, click here. Also, certain countries recognize a United States registration as a basis for filing an application to register a mark in those countries under international treaties….

What are common law rights?
Federal registration is not required to establish rights in a trademark. Common law rights arise from actual use of a mark. Generally, the first to either use a mark in commerce or file an intent to use application with the Patent and Trademark Office has the ultimate right to use and registration. However, there are many benefits of federal trademark registration.

Trademark Glossary

Likelihood of Confusion

Ninth Circuit "Sleekcraft" Factors (from the Ninth Circuit Model Civil Jury Instructions 18.15)

> 1. STRENGTH OR WEAKNESS OF THE PLAINTIFF'S MARK. The more the consuming public recognizes the plaintiff's trademark as an indication of origin of the plaintiff's goods, the more likely it is that consumers would be confused about the source of the defendant's goods if the defendant uses a similar mark.
>
> 2.DEFENDANT'S USE OF THE MARK. If the defendant and plaintiff use their trademarks on the same, related, or complementary kinds of goods there may be a greater likelihood of confusion about the source of the goods than otherwise.
>
> 3. SIMILARITY OF PLAINTIFF'S AND DEFENDANT'S MARKS. If the overall impression created by the plaintiff's trademark in the marketplace is similar to that created by the defendant's trademark in [appearance] [sound] or [meaning], there is a greater chance [that consumers are likely to be confused by defendant's use of a mark] [of likelihood of confusion]. [Similarities in appearance, sound or meaning weigh more heavily than differences in finding the marks are similar].
>
> 4. ACTUAL CONFUSION. If use by the defendant of the plaintiff's trademark has led to instances of actual confusion, this strongly suggests a likelihood of confusion. However actual confusion is not required for a finding of likelihood of confusion. Even if actual confusion did not occur, the defendant's use of the trademark may still be likely to cause confusion, you may conclude that the amount of actual confusion was not substantial. As you consider whether the trademark used by the defendant creates for consumers a likelihood of confusion with the plaintiff's trademark, you should weigh any instances of actual confusion against the opportunities for such confusion. If the instances of actual confusion have been relatively frequent, you may find that there has been substantial actual confusion. If, by contrast, there is a very large volume of sales, but only a few isolated instances of actual confusion you may find that there has not been substantial actual confusion.
>
> 5. DEFENDANT'S INTENT. Knowing use by defendant of the plaintiff's trademark to identify similar goods may strongly show an intent to derive benefit from the reputation of the plaintiff's mark, suggesting an intent to cause a likelihood of confusion. On the other hand, even in the absence of proof that the defendant acted knowingly, the use of plaintiff's trademark to identify similar goods may indicate a likelihood of confusion.
>
> 6. MARKETING/ADVERTISING CHANNELS. If the plaintiff's and defendant's (goods) (services) are likely to be sold in the same or similar stores or

outlets, or advertised in similar media, this may increase the likelihood of confusion.

7. PURCHASER'S DEGREE OF CARE. The more sophisticated the potential buyers of the goods or the more costly the goods, the more careful and discriminating the reasonably prudent purchaser exercising ordinary caution may be. They may be less likely to be confused by similarities in the plaintiff's and defendant's trademarks

8. PRODUCT LINE EXPANSION. When the parties' products differ, you may consider how likely the plaintiff is to begin selling the products for which the defendant is using the plaintiff's trademark. If there is a strong possibility of expanding into the other party's market, there is a greater likelihood of confusion.

Dilution

(1) mark is "famous" = "widely recognized by the general consuming public of the United States"
- advertising/publicity duration/extent/geographic reach
- amount/volume/geographic extent of sales
- actual recognition
- registration?

(2) defendant used in commerce
(3) defendant's use began after the mark became famous
(4) dilution
- blurring = impairs distinctiveness (factors: mark similarity; level of distinctiveness; degree of exclusivity; level of recognition)
- tarnishment = harms reputation

Nominative Use (from New Kids on the Block v. News America Publishing, 971 F.2d 302 (9th Cir. 1992))

(1) "the product or service in question must be one not readily identifiable without use of the trademark"
(2) "only so much of the mark or marks may be used as is reasonably necessary to identify the product or service"
(3) "the user must do nothing that would, in conjunction with the mark, suggest sponsorship or endorsement by the trademark holder"

Uniform Dispute Resolution Procedure

(1) the domain name is confusing similar (or identical) to a third party's mark
(2) the registrant has no legitimate interests in the name

But registrant can show legitimate rights by:
- actual or planned bona fide offering of goods/services;

- it is commonly known by the domain name; or
- making a legitimate noncommercial or fair use without intent for commercial gain, misleading diversion of traffic, or dilution.

(3) the name is being used in bad faith:
- acquired the name for profitable resale;
- registered the name to block the legitimate TM owner if a pattern can be shown;
- acquired name to disrupt a competitor; or
- name is intended to attract attention to site by creating a likelihood of confusion.

Anticybersquatting Consumer Protection Act

(1) Domain name registrant registers a domain name containing a third party trademark
(2) has a bad faith intent to profit from the domain name
- the registrant's IP rights in the domain name
- if the domain name contains the registrant's real name
- the use of the domain name in a bona fide offering of goods/services
- a bona fide noncommercial or fair use of the domain name
- an intent to divert consumers in a way that harms the trademark owner's goodwill
- an offer to sell the domain name without having used it for a bona fide offering of goods/services
- providing false contact info
- multiple bogus registrations
- distinctiveness/famousness of the mark

(3) registers, traffics in or uses a domain name that is identical or confusingly similar to the mark or, in the case of a famous mark, dilutes it.

15 U.S.C. § 1125. False designations of origin, false descriptions, and dilution forbidden

(a) Civil action

(1) Any person who, on or in connection with any goods or services, or any container for goods, uses in commerce any word, term, name, symbol, or device, or any combination thereof, or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact, which—

(A) is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person, or

(B) in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his or her or another person's goods, services, or commercial activities,

shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act.

(2) As used in this subsection, the term "any person" includes any State, instrumentality of a State or employee of a State or instrumentality of a State acting in his or her official capacity. Any State, and any such instrumentality, officer, or employee, shall be subject to the provisions of this chapter in the same manner and to the same extent as any nongovernmental entity.

(3) In a civil action for trade dress infringement under this chapter for trade dress not registered on the principal register, the person who asserts trade dress protection has the burden of proving that the matter sought to be protected is not functional.

(b) Importation

Any goods marked or labeled in contravention of the provisions of this section shall not be imported into the United States or admitted to entry at any customhouse of the United States. The owner, importer, or consignee of goods refused entry at any customhouse under this section may have any recourse by protest or appeal that is given under the customs revenue laws or may have the remedy given by this chapter in cases involving goods refused entry or seized.

(c) Dilution by blurring; dilution by tarnishment

(1) Injunctive relief

Subject to the principles of equity, the owner of a famous mark that is distinctive, inherently or through acquired distinctiveness, shall be entitled to an injunction against another person who, at any time after the owner's mark has become famous, commences use of a mark or trade name in commerce that is likely to cause dilution by blurring or dilution by tarnishment of the famous mark, regardless of the presence or absence of actual or likely confusion, of competition, or of actual economic injury.

(2) Definitions

(A) For purposes of paragraph (1), a mark is famous if it is widely recognized by the general consuming public of the United States as

a designation of source of the goods or services of the mark's owner. In determining whether a mark possesses the requisite degree of recognition, the court may consider all relevant factors, including the following:

(i) The duration, extent, and geographic reach of advertising and publicity of the mark, whether advertised or publicized by the owner or third parties.

(ii) The amount, volume, and geographic extent of sales of goods or services offered under the mark.

(iii) The extent of actual recognition of the mark.

(iv) Whether the mark was registered under the Act of March 3, 1881, or the Act of February 20, 1905, or on the principal register.

(B) For purposes of paragraph (1), "dilution by blurring" is association arising from the similarity between a mark or trade name and a famous mark that impairs the distinctiveness of the famous mark. In determining whether a mark or trade name is likely to cause dilution by blurring, the court may consider all relevant factors, including the following:

(i) The degree of similarity between the mark or trade name and the famous mark.

(ii) The degree of inherent or acquired distinctiveness of the famous mark.

(iii) The extent to which the owner of the famous mark is engaging in substantially exclusive use of the mark.

(iv) The degree of recognition of the famous mark.

(v) Whether the user of the mark or trade name intended to create an association with the famous mark.

(vi) Any actual association between the mark or trade name and the famous mark.

(C) For purposes of paragraph (1), "dilution by tarnishment" is association arising from the similarity between a mark or trade name and a famous mark that harms the reputation of the famous mark.

(3) Exclusions

The following shall not be actionable as dilution by blurring or dilution by tarnishment under this subsection:

(A) Any fair use, including a nominative or descriptive fair use, or facilitation of such fair use, of a famous mark by another person other than as a designation of source for the person's own goods or services, including use in connection with—

(i) advertising or promotion that permits consumers to compare goods or services; or

(ii) identifying and parodying, criticizing, or commenting upon the famous mark owner or the goods or services of the famous mark owner.

(B) All forms of news reporting and news commentary.

(C) Any noncommercial use of a mark.

(4) Burden of proof

In a civil action for trade dress dilution under this chapter for trade dress not registered on the principal register, the person who asserts trade dress protection has the burden of proving that—

(A) the claimed trade dress, taken as a whole, is not functional and is famous; and

(B) if the claimed trade dress includes any mark or marks registered on the principal register, the unregistered matter, taken as a whole, is famous separate and apart from any fame of such registered marks.

(5) Additional remedies

In an action brought under this subsection, the owner of the famous mark shall be entitled to injunctive relief as set forth in section 1116 of this title. The owner of the famous mark shall also be entitled to the remedies set forth in sections 1117 (a) and 1118 of this title, subject to the discretion of the court and the principles of equity if—

(A) the mark or trade name that is likely to cause dilution by blurring or dilution by tarnishment was first used in commerce by the person against whom the injunction is sought after October 6, 2006; and

(B) in a claim arising under this subsection—

(i) by reason of dilution by blurring, the person against whom the injunction is sought willfully intended to trade on the recognition of the famous mark; or

(ii) by reason of dilution by tarnishment, the person against whom the injunction is sought willfully intended to harm the reputation of the famous mark.

(6) Ownership of valid registration a complete bar to action

The ownership by a person of a valid registration under the Act of March 3, 1881, or the Act of February 20, 1905, or on the principal register under this chapter shall be a complete bar to an action against that person, with respect to that mark, that—

(A)

(i) is brought by another person under the common law or a statute of a State; and

(ii) seeks to prevent dilution by blurring or dilution by tarnishment; or

(B) asserts any claim of actual or likely damage or harm to the distinctiveness or reputation of a mark, label, or form of advertisement.

(7) Savings clause

Nothing in this subsection shall be construed to impair, modify, or supersede the applicability of the patent laws of the United States.

(d) Cyberpiracy prevention

(1)

(A) A person shall be liable in a civil action by the owner of a mark, including a personal name which is protected as a mark under this section, if, without regard to the goods or services of the parties, that person—

(i) has a bad faith intent to profit from that mark, including a personal name which is protected as a mark under this section; and

(ii) registers, traffics in, or uses a domain name that—

(I) in the case of a mark that is distinctive at the time of registration of the domain name, is identical or confusingly similar to that mark;

(II) in the case of a famous mark that is famous at the time of registration of the domain name, is identical or confusingly similar to or dilutive of that mark; or

(III) is a trademark, word, or name protected by reason of section 706 of title 18 or section 220506 of title 36.

(B)

(i) In determining whether a person has a bad faith intent described under subparagraph (A), a court may consider factors such as, but not limited to—

(I) the trademark or other intellectual property rights of the person, if any, in the domain name;

(II) the extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person;

(III) the person’s prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;

(IV) the person’s bona fide noncommercial or fair use of the mark in a site accessible under the domain name;

(V) the person’s intent to divert consumers from the mark owner’s online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site;

(VI) the person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct;

(VII) the person's provision of material and misleading false contact information when applying for the registration of the domain name, the person's intentional failure to maintain accurate contact information, or the person's prior conduct indicating a pattern of such conduct;

(VIII) the person's registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties; and

(IX) the extent to which the mark incorporated in the person's domain name registration is or is not distinctive and famous within the meaning of subsection (c).

(ii) Bad faith intent described under subparagraph (A) shall not be found in any case in which the court determines that the person believed and had reasonable grounds to believe that the use of the domain name was a fair use or otherwise lawful.

(C) In any civil action involving the registration, trafficking, or use of a domain name under this paragraph, a court may order the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark.

(D) A person shall be liable for using a domain name under subparagraph (A) only if that person is the domain name registrant or that registrant's authorized licensee.

(E) As used in this paragraph, the term "traffics in" refers to transactions that include, but are not limited to, sales, purchases, loans, pledges, licenses, exchanges of currency, and any other transfer for consideration or receipt in exchange for consideration.

(2)

(A) The owner of a mark may file an in rem civil action against a domain name in the judicial district in which the domain name registrar, domain name registry, or other domain name authority that registered or assigned the domain name is located if—

(i) the domain name violates any right of the owner of a mark registered in the Patent and Trademark Office, or protected under subsection (a) or (c) of this section; and

(ii) the court finds that the owner—

(I) is not able to obtain in personam jurisdiction over a person who would have been a defendant in a civil action under paragraph (1); or

(II) through due diligence was not able to find a person who would have been a defendant in a civil action under paragraph (1) by—

(aa) sending a notice of the alleged violation and intent to proceed under this paragraph to the registrant of the domain name at the postal and e-mail address provided by the registrant to the registrar; and

(bb) publishing notice of the action as the court may direct promptly after filing the action.

(B) The actions under subparagraph (A)(ii) shall constitute service of process.

(C) In an in rem action under this paragraph, a domain name shall be deemed to have its situs in the judicial district in which—

(i) the domain name registrar, registry, or other domain name authority that registered or assigned the domain name is located; or

(ii) documents sufficient to establish control and authority regarding the disposition of the registration and use of the domain name are deposited with the court.

(D)

(i) The remedies in an in rem action under this paragraph shall be limited to a court order for the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark. Upon receipt of written notification of a filed, stamped copy of a complaint filed by the owner of a mark in a United States district court under this paragraph, the domain name registrar, domain name registry, or other domain name authority shall—

(I) expeditiously deposit with the court documents sufficient to establish the court's control and authority regarding the disposition of the registration and use of the domain name to the court; and

(II) not transfer, suspend, or otherwise modify the domain name during the pendency of the action, except upon order of the court.

(ii) The domain name registrar or registry or other domain name authority shall not be liable for injunctive or monetary relief under this paragraph except in the case of bad faith or reckless disregard, which includes a willful failure to comply with any such court order.

(3) The civil action established under paragraph (1) and the in rem action established under paragraph (2), and any remedy available under either such action, shall be in addition to any other civil action or remedy otherwise applicable.
(4) The in rem jurisdiction established under paragraph (2) shall be in addition to any other jurisdiction that otherwise exists, whether in rem or in personam.

15 U.S.C. § 8131. Cyberpiracy protections for individuals

(1) In general

(A) Civil liability

Any person who registers a domain name that consists of the name of another living person, or a name substantially and confusingly similar thereto, without that person's consent, with the specific intent to profit from such name by selling the domain name for financial gain to that person or any third party, shall be liable in a civil action by such person.

(B) Exception

A person who in good faith registers a domain name consisting of the name of another living person, or a name substantially and confusingly similar thereto, shall not be liable under this paragraph if such name is used in, affiliated with, or related to a work of authorship protected under Title 17, including a work made for hire as defined in section 101 of Title 17, and if the person registering the domain name is the copyright owner or licensee of the work, the person intends to sell the domain name in conjunction with the lawful exploitation of the work, and such registration is not prohibited by a contract between the registrant and the named person. The exception under this subparagraph shall apply only to a civil action brought under paragraph (1) and shall in no manner limit the protections afforded under the Trademark Act of 1946 (15 U.S.C. 1051 et seq.) or other provision of Federal or State law.

(2) Remedies

In any civil action brought under paragraph (1), a court may award injunctive relief, including the forfeiture or cancellation of the domain name or the transfer of the domain name to the plaintiff. The court may also, in its discretion, award costs and attorneys fees to the prevailing party.

(3) Definition

In this section, the term "domain name" has the meaning given that term in section 45 of the Trademark Act of 1946 (15 U.S.C. 1127).

(4) Effective date

This section shall apply to domain names registered on or after November 29, 1999.

15 U.S.C. § 1114. Remedies; infringement; innocent infringement by printers and publishers

(1) Any person who shall, without the consent of the registrant—

(a) use in commerce any reproduction, counterfeit, copy, or colorable imitation of a registered mark in connection with the sale, offering for sale, distribution, or advertising of any goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive; or

(b) reproduce, counterfeit, copy, or colorably imitate a registered mark and apply such reproduction, counterfeit, copy, or colorable imitation to labels, signs, prints, packages, wrappers, receptacles or advertisements intended to be used in commerce upon or in connection with the sale, offering for sale, distribution, or advertising of goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive,

shall be liable in a civil action by the registrant for the remedies hereinafter provided. Under subsection (b) hereof, the registrant shall not be entitled to recover profits or damages unless the acts have been committed with knowledge that such imitation is intended to be used to cause confusion, or to cause mistake, or to deceive.

As used in this paragraph, the term "any person" includes the United States, all agencies and instrumentalities thereof, and all individuals, firms, corporations, or other persons acting for the United States and with the authorization and consent of the United States, and any State, any instrumentality of a State, and any officer or employee of a State or instrumentality of a State acting in his or her official capacity. The United States, all agencies and instrumentalities thereof, and all individuals, firms, corporations, other persons acting for the United States and with the authorization and consent of the United States, and any State, and any such instrumentality, officer, or employee, shall be subject to the provisions of this chapter in the same manner and to the same extent as any nongovernmental entity.

(2) Notwithstanding any other provision of this chapter, the remedies given to the owner of a right infringed under this chapter or to a person bringing an action under section 1125 (a) or (d) of this title shall be limited as follows:

(A) Where an infringer or violator is engaged solely in the business of printing the mark or violating matter for others and establishes that he or she was an innocent infringer or innocent violator, the owner of the right infringed or person bringing the action under section 1125(a) of this title shall be entitled as against such infringer or violator only to an injunction against future printing.

(B) Where the infringement or violation complained of is contained in or is part of paid advertising matter in a newspaper, magazine, or other similar periodical or in an electronic communication as defined in section 2510 (12) of title 18, the remedies of the owner of the right infringed or person bringing the action under section 1125(a) of this title as against the publisher or distributor of such newspaper, magazine, or other similar periodical or electronic communication shall be limited to an injunction against the presentation of such advertising

matter in future issues of such newspapers, magazines, or other similar periodicals or in future transmissions of such electronic communications. The limitations of this subparagraph shall apply only to innocent infringers and innocent violators.
(C) Injunctive relief shall not be available to the owner of the right infringed or person bringing the action under section 1125(a) of this title with respect to an issue of a newspaper, magazine, or other similar periodical or an electronic communication containing infringing matter or violating matter where restraining the dissemination of such infringing matter or violating matter in any particular issue of such periodical or in an electronic communication would delay the delivery of such issue or transmission of such electronic communication after the regular time for such delivery or transmission, and such delay would be due to the method by which publication and distribution of such periodical or transmission of such electronic communication is customarily conducted in accordance with sound business practice, and not due to any method or device adopted to evade this section or to prevent or delay the issuance of an injunction or restraining order with respect to such infringing matter or violating matter.
(D)
(i)

(I) A domain name registrar, a domain name registry, or other domain name registration authority that takes any action described under clause (ii) affecting a domain name shall not be liable for monetary relief or, except as provided in subclause (II), for injunctive relief, to any person for such action, regardless of whether the domain name is finally determined to infringe or dilute the mark.
(II) A domain name registrar, domain name registry, or other domain name registration authority described in subclause (I) may be subject to injunctive relief only if such registrar, registry, or other registration authority has—

(aa) not expeditiously deposited with a court, in which an action has been filed regarding the disposition of the domain name, documents sufficient for the court to establish the court's control and authority regarding the disposition of the registration and use of the domain name;
(bb) transferred, suspended, or otherwise modified the domain name during the pendency of the action, except upon order of the court; or
(cc) willfully failed to comply with any such court order.

(ii) An action referred to under clause (i)(I) is any action of refusing to register, removing from registration, transferring, temporarily disabling, or permanently canceling a domain name—

(I) in compliance with a court order under section 1125(d) of this title; or

(II) in the implementation of a reasonable policy by such registrar, registry, or authority prohibiting the registration of a domain name that is identical to, confusingly similar to, or dilutive of another's mark.

(iii) A domain name registrar, a domain name registry, or other domain name registration authority shall not be liable for damages under this section for the registration or maintenance of a domain name for another absent a showing of bad faith intent to profit from such registration or maintenance of the domain name.

(iv) If a registrar, registry, or other registration authority takes an action described under clause (ii) based on a knowing and material misrepresentation by any other person that a domain name is identical to, confusingly similar to, or dilutive of a mark, the person making the knowing and material misrepresentation shall be liable for any damages, including costs and attorney's fees, incurred by the domain name registrant as a result of such action. The court may also grant injunctive relief to the domain name registrant, including the reactivation of the domain name or the transfer of the domain name to the domain name registrant.

(v) A domain name registrant whose domain name has been suspended, disabled, or transferred under a policy described under clause (ii)(II) may, upon notice to the mark owner, file a civil action to establish that the registration or use of the domain name by such registrant is not unlawful under this chapter. The court may grant injunctive relief to the domain name registrant, including the reactivation of the domain name or transfer of the domain name to the domain name registrant.

(E) As used in this paragraph—

(i) the term "violator" means a person who violates section 1125 (a) of this title; and

(ii) the term "violating matter" means matter that is the subject of a violation under section 1125 (a) of this title.

(3)

(A) Any person who engages in the conduct described in paragraph (11) of section 110 of title 17 and who complies with the requirements set forth in that paragraph is not liable on account of such conduct for a violation of any right under this chapter. This subparagraph does not preclude liability, nor shall it be construed to restrict the defenses or limitations on rights granted under this chapter, of a person for conduct not described in paragraph (11) of section 110 of title 17, even if that person also engages in conduct described in paragraph (11) of section 110 of such title.

(B) A manufacturer, licensee, or licensor of technology that enables the making of limited portions of audio or video content of a motion picture imperceptible as described in subparagraph (A) is not liable on account of such manufacture or license for a violation of any right under this chapter, if such manufacturer, licensee, or licensor ensures that the technology provides a clear and conspicuous notice at the beginning of each performance that the performance of the motion picture is altered from the performance intended by the director or copyright holder of the motion picture. The limitations on liability in subparagraph (A) and

this subparagraph shall not apply to a manufacturer, licensee, or licensor of technology that fails to comply with this paragraph.
(C) The requirement under subparagraph (B) to provide notice shall apply only with respect to technology manufactured after the end of the 180-day period beginning on April 27, 2005.
(D) Any failure by a manufacturer, licensee, or licensor of technology to qualify for the exemption under subparagraphs (A) and (B) shall not be construed to create an inference that any such party that engages in conduct described in paragraph (11) of section 110 of title 17 is liable for trademark infringement by reason of such conduct.

UDRP Rules

[Editor's note: In years past, I have included copies of the UDRP Uniform Domain Name Dispute Resolution Policy and Rules for Uniform Domain Name Dispute Resolution Policy in the course materials. To save paper, I will simply point you to review them at your leisure if you are interested.

The policy: http://www.icann.org/en/udrp/udrp-policy-24oct99.htm
The rules: http://www.icann.org/en/dndr/udrp/uniform-rules.htm]

Lamparello v. Falwell, 420 F.3d 309 (4th Cir. 2005).
Motz, Circuit Judge.

Christopher Lamparello appeals the district court's order enjoining him from maintaining a gripe website critical of Reverend Jerry Falwell. For the reasons stated below, we reverse.

I.

Reverend Falwell is "a nationally known minister who has been active as a commentator on politics and public affairs." He holds the common law trademarks "Jerry Falwell" and "Falwell," and the registered trademark "Listen America with Jerry Falwell." Jerry Falwell Ministries can be found online at "www.falwell.com," a website which receives 9,000 hits (or visits) per day.

Lamparello registered the domain name "www.fallwell.com" on February 11, 1999, after hearing Reverend Falwell give an interview "in which he expressed opinions about gay people and homosexuality that [Lamparello] considered ... offensive." Lamparello created a website at that domain name to respond to what he believed were "untruths about gay people." Lamparello's website included headlines such as "Bible verses that Dr. Falwell chooses to ignore" and "Jerry Falwell has been bearing false witness (Exodus 20:16) against his gay and lesbian neighbors for a long time." The site also contained in-depth criticism of Reverend Falwell's views. For example, the website stated:

> Dr. Falwell says that he is on the side of truth. He says that he will preach that homosexuality is a sin until the day he dies. But we believe that if the reverend were to take another thoughtful look at the scriptures, he would discover that they have been twisted around to support an anti-gay political agenda ... at the expense of the gospel.

Although the interior pages of Lamparello's website did not contain a disclaimer, the homepage prominently stated, "This website is NOT affiliated with Jerry Falwell or his ministry"; advised, "If you would like to visit Rev. Falwell's website, you may click here"; and provided a hyperlink to Reverend Falwell's website.

At one point, Lamparello's website included a link to the Amazon.com webpage for a book that offered interpretations of the Bible that Lamparello favored, but the parties agree that Lamparello has never sold goods or services on his website. The parties also agree that "Lamparello's domain name and web site at www.fallwell.com," which received only 200 hits per day, "had no measurable impact on the quantity of visits to [Reverend Falwell's] web site at www.falwell.com."

Nonetheless, Reverend Falwell sent Lamparello letters in October 2001 and June 2003 demanding that he cease and desist from using www.fallwell.com or any variation of Reverend Falwell's name as a domain name. Ultimately, Lamparello filed this action against Reverend Falwell and his ministries (collectively referred to hereinafter as "Reverend Falwell"), seeking a declaratory judgment of noninfringement. Reverend Falwell counter-claimed, alleging trademark infringement under 15 U.S.C. § 1114 (2000), false designation of origin under 15 U.S.C. §

1125(a), unfair competition under 15 U.S.C. § 1126 and the common law of Virginia,[1] and cybersquatting under 15 U.S.C. § 1125(d).

The parties stipulated to all relevant facts and filed cross-motions for summary judgment. The district court granted summary judgment to Reverend Falwell, enjoined Lamparello from using Reverend Falwell's mark at www.fallwell.com, and required Lamparello to transfer the domain name to Reverend Falwell. However, the court denied Reverend Falwell's request for statutory damages or attorney fees, reasoning that the "primary motive" of Lamparello's website was "to put forth opinions on issues that were contrary to those of [Reverend Falwell]" and "not to take away monies or to profit."

Lamparello appeals the district court's order; Reverend Falwell cross-appeals the denial of statutory damages and attorney fees. We review de novo a district court's ruling on cross-motions for summary judgment. See People for the Ethical Treatment of Animals v. Doughney, 263 F.3d 359, 364 (4th Cir. 2001) [hereinafter "PETA"].

II.

We first consider Reverend Falwell's claims of trademark infringement and false designation of origin.

A….

Both infringement and false designation of origin have five elements. To prevail under either cause of action, the trademark holder must prove:

> (1) that it possesses a mark; (2) that the [opposing party] used the mark; (3) that the [opposing party's] use of the mark occurred "in commerce"; (4) that the [opposing party] used the mark "in connection with the sale, offering for sale, distribution, or advertising" of goods or services; and (5) that the [opposing party] used the mark in a manner likely to confuse consumers.

Trademark law serves the important functions of protecting product identification, providing consumer information, and encouraging the production of quality goods and services. See Qualitex Co. v. Jacobson Prods. Co., 514 U.S. 159, 164 (1995). But protections "'against unfair competition'" cannot be transformed into "'rights to control language.'" "Such a transformation" would raise serious First Amendment concerns because it would limit the

> ability to discuss the products or criticize the conduct of companies that may be of widespread public concern and importance. Much useful social and commercial discourse would be all but impossible if speakers were under threat of an

[1] …because "[t]he test for trademark infringement and unfair competition under the Lanham Act is essentially the same as that for common law unfair competition under Virginia law because both address the likelihood of confusion as to the source of the goods or services involved," Reverend Falwell's state-law unfair competition claim rises or falls with his federal claims of infringement and false designation of origin. Therefore, we will not analyze his state-law claim separately.

> infringement lawsuit every time they made reference to a person, company or product by using its trademark.

Lamparello and his amici argue at length that application of the Lanham Act must be restricted to "commercial speech" to assure that trademark law does not become a tool for unconstitutional censorship. The Sixth Circuit has endorsed this view, see Taubman Co. v. Webfeats, 319 F.3d 770, 774 (6th Cir. 2003), and the Ninth Circuit recently has done so as well, see Bosley Med. Inst., Inc. v. Kremer, 403 F.3d 672, 674 (9th Cir. 2005).

In its two most significant recent amendments to the Lanham Act, the Federal Trademark Dilution Act of 1995 ("FTDA") and the Anticybersquatting Consumer Protection Act of 1999 ("ACPA"), Congress left little doubt that it did not intend for trademark laws to impinge the First Amendment rights of critics and commentators. The dilution statute applies to only a "commercial use in commerce of a mark," and explicitly states that the "[n]oncommercial use of a mark" is not actionable. Congress explained that this language was added to "adequately address [ ] legitimate First Amendment concerns," and "incorporate[d] the concept of 'commercial' speech from the 'commercial speech' doctrine." Similarly, Congress directed that in determining whether an individual has engaged in cybersquatting, the courts may consider whether the person's use of the mark is a "bona fide noncommercial or fair use." The legislature believed this provision necessary to "protect[ ] the rights of Internet users and the interests of all Americans in free speech and protected uses of trademarked names for such things as parody, comment, criticism, comparative advertising, news reporting, etc."

In contrast, the trademark infringement and false designation of origin provisions of the Lanham Act (Sections 32 and 43(a), respectively) do not employ the term "noncommercial." They do state, however, that they pertain only to the use of a mark "in connection with the sale, offering for sale, distribution, or advertising of any goods or services," or "in connection with any goods or services." But courts have been reluctant to define those terms narrowly.[2] Rather, as the Second Circuit has explained, "[t]he term 'services' has been interpreted broadly" and so "[t]he Lanham Act has ... been applied to defendants furnishing a wide variety of non-commercial public and civic benefits." Similarly, in *PETA* we noted that a website need not actually sell goods or services for the use of a mark in that site's domain name to constitute a use "'in connection with' goods or services." PETA, 263 F.3d at 365; see also Taubman Co., 319 F.3d at 775 (concluding that website with two links to websites of for-profit entities violated the Lanham Act).

Thus, even if we accepted Lamparello's contention that Sections 32 and 43(a) of the Lanham Act apply only to commercial speech, we would still face the difficult question of what constitutes such speech under those provisions. In the case at hand, we need not resolve that question or determine whether Sections 32 and 43(a) apply exclusively to commercial speech because Reverend Falwell's claims of trademark infringement and false designation fail for a more obvious reason. The hallmark of such claims is a likelihood of confusion-and there is no likelihood of confusion here.

[2] Indeed, Lamparello agreed at oral argument that the Lanham Act's prohibitions on infringement and false designation apply to more than just commercial speech as defined by the Supreme Court.

B.

1.

"[T]he use of a competitor's mark that does not cause confusion as to source is permissible." Dorr-Oliver, Inc. v. Fluid-Quip, Inc., Accordingly, Lamparello can only be liable for infringement and false designation if his use of Reverend Falwell's mark would be likely to cause confusion as to the source of the website found at www.fallwell.com. This likelihood-of-confusion test "generally strikes a comfortable balance" between the First Amendment and the rights of markholders.

We have identified seven factors helpful in determining whether a likelihood of confusion exists as to the source of a work, but "not all these factors are always relevant or equally emphasized in each case." The factors are: "(a) the strength or distinctiveness of the mark; (b) the similarity of the two marks; (c) the similarity of the goods/services the marks identify; (d) the similarity of the facilities the two parties use in their businesses; (e) the similarity of the advertising used by the two parties; (f) the defendant's intent; (g) actual confusion."

Reverend Falwell's mark is distinctive, and the domain name of Lamparello's website, www.fallwell.com, closely resembles it. But, although Lamparello and Reverend Falwell employ similar marks online, Lamparello's website looks nothing like Reverend Falwell's; indeed, Lamparello has made no attempt to imitate Reverend Falwell's website. Moreover, Reverend Falwell does not even argue that Lamparello's website constitutes advertising or a facility for business, let alone a facility or advertising similar to that of Reverend Falwell. Furthermore, Lamparello clearly created his website intending only to provide a forum to criticize ideas, not to steal customers.

Most importantly, Reverend Falwell and Lamparello do not offer similar goods or services. Rather they offer opposing ideas and commentary. Reverend Falwell's mark identifies his spiritual and political views; the website at www.fallwell.com criticizes those very views. After even a quick glance at the content of the website at www.fallwell.com, no one seeking Reverend Falwell's guidance would be misled by the domain name—www.fallwell.com—into believing Reverend Falwell authorized the content of that website. No one would believe that Reverend Falwell sponsored a site criticizing himself, his positions, and his interpretations of the Bible.[3]

Finally, the fact that people contacted Reverend Falwell's ministry to report that they found the content at www.fallwell.com antithetical to Reverend Falwell's views does not illustrate, as Reverend Falwell claims, that the website engendered actual confusion. To the contrary, the anecdotal evidence Reverend Falwell submitted shows that those searching for Reverend Falwell's site and arriving instead at Lamparello's site quickly realized that Reverend Falwell was not the source of the content therein.

[3] If Lamparello had neither criticized Reverend Falwell by name nor expressly rejected Reverend Falwell's teachings, but instead simply had quoted Bible passages and offered interpretations of them subtly different from those of Reverend Falwell, this would be a different case. For, while a gripe site, or a website dedicated to criticism of the markholder, will seldom create a likelihood of confusion, a website purporting to be the official site of the markholder and, for example, articulating positions that could plausibly have come from the markholder may well create a likelihood of confusion.

For all of these reasons, it is clear that the undisputed record evidences no likelihood of confusion. In fact, Reverend Falwell even conceded at oral argument that those viewing the content of Lamparello's website probably were unlikely to confuse Reverend Falwell with the source of that material.

2.

Nevertheless, Reverend Falwell argues that he is entitled to prevail under the "initial interest confusion" doctrine. This relatively new and sporadically applied doctrine holds that "the Lanham Act forbids a competitor from luring potential customers away from a producer by initially passing off its goods as those of the producer's, even if confusion as to the source of the goods is dispelled by the time any sales are consummated." According to Reverend Falwell, this doctrine requires us to compare his mark with Lamparello's website domain name, www.fallwell.com, *without* considering the content of Lamparello's website. Reverend Falwell argues that some people who misspell his name may go to www.fallwell.com assuming it is his site, thus giving Lamparello an unearned audience-albeit one that quickly disappears when it realizes it has not reached Reverend Falwell's site. This argument fails for two reasons.

First, we have never adopted the initial interest confusion theory; rather, we have followed a very different mode of analysis, requiring courts to determine whether a likelihood of confusion exists by "examin[ing] the allegedly infringing use *in the context in which it is seen by the ordinary consumer*."

Contrary to Reverend Falwell's arguments, we did not abandon this approach in *PETA*. Our inquiry in *PETA* was limited to whether Doughney's use of the domain name "www.peta.org" constituted a successful enough parody of People for the Ethical Treatment of Animals that no one was likely to believe www.peta.org was sponsored or endorsed by that organization. For a parody to be successful, it "must convey two simultaneous—and contradictory—messages: that it is the original, but also that it is not the original and is instead a parody." Doughney argued that his domain name conveyed the first message (that it was PETA's website) and that the content of his website conveyed the requisite second message (that it was not PETA's site). Although "[t]he website's content ma[de] it clear that it [wa]s not related to PETA," we concluded that the website's content could not convey the requisite second message because the site's content "[wa]s not conveyed *simultaneously* with the first message, [i.e., the domain name itself,] as required to be considered a parody." Accordingly, we found the "district court properly rejected Doughney's parody defense."

PETA simply outlines the parameters of the parody defense; it does not adopt the initial interest confusion theory or otherwise diminish the necessity of examining context when determining whether a likelihood of confusion exists. Indeed, in *PETA* itself, rather than embracing a new approach, we reiterated that "[t]o determine whether a likelihood of confusion exists, a court should not consider how closely a *fragment* of a given use duplicates the trademark, but must instead consider *whether the use in its entirety creates a likelihood of confusion*." (emphasis added). When dealing with domain names, this means a court must evaluate an allegedly

infringing domain name in conjunction with the content of the website identified by the domain name.[4]

Moreover, even if we did endorse the initial interest confusion theory, that theory would not assist Reverend Falwell here because it provides no basis for liability in circumstances such as these. The few appellate courts that have followed the Ninth Circuit and imposed liability under this theory for using marks on the Internet have done so only in cases involving a factor utterly absent here—one business's use of another's mark for its own financial gain.

Profiting financially from initial interest confusion is thus a key element for imposition of liability under this theory.[5] When an alleged infringer does not compete with the markholder for sales, "some initial confusion will not likely facilitate free riding on the goodwill of another mark, or otherwise harm the user claiming infringement. Where confusion has little or no meaningful effect in the marketplace, it is of little or no consequence in our analysis." For this reason, even the Ninth Circuit has stated that a firm is not liable for using another's mark in its domain name if it "could not financially capitalize on [a] misdirected consumer [looking for the markholder's site] even if it so desired."

This critical element—use of another firm's mark to capture the markholder's customers and profits—simply does not exist when the alleged infringer establishes a gripe site that criticizes the markholder. See Hannibal Travis, The Battle For Mindshare: The Emerging Consensus that the First Amendment Protects Corporate Criticism and Parody on the Internet, 10 Va. J.L. & Tech. 3, 85 (Winter 2005) ("The premise of the 'initial interest' confusion cases is that by using the plaintiff's trademark to divert its customers, the defendant is engaging in the old 'bait and switch.' But because ... Internet users who find [gripe sites] are not sold anything, the mark may be the 'bait,' but there is simply no 'switch.'") (citations omitted).[6] Applying the initial interest confusion theory to gripe sites like Lamparello's would enable the markholder to insulate himself from criticism—or at least to minimize access to it. We have already condemned such uses of the Lanham Act, stating that a markholder cannot "'shield itself from criticism by

[4] Contrary to Reverend Falwell's suggestions, this rule does not change depending on how similar the domain name or title is to the mark. Hence, Reverend Falwell's assertion that he objects only to Lamparello using the domain name www.fallwell.com and has no objection to Lamparello posting his criticisms at "www.falwelliswrong.com," or a similar domain name, does not entitle him to a different evaluation rule. Rather it has long been established that even when alleged infringers use the very marks at issue in titles, courts look to the underlying content to determine whether the titles create a likelihood of confusion as to source.

[5] Offline uses of marks found to cause actionable initial interest confusion also have involved financial gain. And even those courts recognizing the initial interest confusion theory of liability but finding no actionable initial confusion involved one business's use of another's mark for profit.

[6] Although the appellate courts that have adopted the initial interest confusion theory have only applied it to profit-seeking uses of another's mark, the district courts have not so limited the application of the theory. Without expressly referring to this theory, two frequently-discussed district court cases have held that using another's domain name to post content antithetical to the markholder constitutes infringement. See Planned Parenthood Fed'n of Am., Inc. v. Bucci, 1997 WL 133313 (S.D.N.Y. March 24, 1997), aff'd, 152 F.3d 920 (2d Cir. 1998) (table) (finding use of domain name "www.plannedparenthood.com" to provide links to passages of anti-abortion book constituted infringement); Jews for Jesus v. Brodsky, 993 F. Supp. 282 (D. N.J. 1998), aff'd, 159 F.3d 1351 (3d Cir. 1998) (table) (finding use of "www.jewsforjesus.org" to criticize religious group constituted infringement). We think both cases were wrongly decided to the extent that in determining whether the domain names were confusing, the courts did not consider whether the websites' content would dispel any confusion. In expanding the initial interest confusion theory of liability, these cases cut it off from its moorings to the detriment of the First Amendment.

forbidding the use of its name in commentaries critical of its conduct.'" "[J]ust because speech is critical of a corporation and its business practices is not a sufficient reason to enjoin the speech."

In sum, even if we were to accept the initial interest confusion theory, that theory would not apply in the case at hand. Rather, to determine whether a likelihood of confusion exists as to the source of a gripe site like that at issue in this case, a court must look not only to the allegedly infringing domain name, but also to the underlying content of the website. When we do so here, it is clear, as explained above, that no likelihood of confusion exists. Therefore, the district court erred in granting Reverend Falwell summary judgment on his infringement, false designation, and unfair competition claims.

III.

We evaluate Reverend Falwell's cybersquatting claim separately because the elements of a cybersquatting violation differ from those of traditional Lanham Act violations. To prevail on a cybersquatting claim, Reverend Falwell must show that Lamparello: (1) "had a bad faith intent to profit from using the [www.fallwell.com] domain name," and (2) the domain name www.fallwell.com "is identical or confusingly similar to, or dilutive of, the distinctive and famous [Falwell] mark."

"The paradigmatic harm that the ACPA was enacted to eradicate" is "the practice of cybersquatters registering several hundred domain names in an effort to sell them to the legitimate owners of the mark." Lucas Nursery & Landscaping, Inc. v. Grosse, 359 F.3d 806, 810 (6th Cir. 2004). The Act was also intended to stop the registration of multiple marks with the hope of selling them to the highest bidder, "distinctive marks to defraud consumers" or "to engage in counterfeiting activities," and "well-known marks to prey on consumer confusion by misusing the domain name to divert customers from the mark owner's site to the cybersquatter's own site, many of which are pornography sites that derive advertising revenue based on the number of visits, or 'hits,' the site receives." S.Rep. No. 106-140. The Act was not intended to prevent "noncommercial uses of a mark, such as for comment, criticism, parody, news reporting, etc.," and thus they "are beyond the scope" of the ACPA.

To distinguish abusive domain name registrations from legitimate ones, the ACPA directs courts to consider nine nonexhaustive factors [the court then quotes the statute]….

These factors attempt "to balance the property interests of trademark owners with the legitimate interests of Internet users and others who seek to make lawful uses of others' marks, including for purposes such as comparative advertising, *comment, criticism*, parody, news reporting, fair use, etc." H.R. Rep. No. 106-412 (emphasis added). "The first four [factors] suggest circumstances that may tend to indicate an absence of bad-faith intent to profit from the goodwill of a mark, and the others suggest circumstances that may tend to indicate that such bad-faith intent exists." Id. However, "[t]here is no simple formula for evaluating and weighing these factors. For example, courts do not simply count up which party has more factors in its favor after the evidence is in." In fact, because use of these listed factors is permissive, "[w]e need not ... march through" them all in every case. "The factors are given to courts as a guide, not as a

substitute for careful thinking about whether the conduct at issue is motivated by a bad faith intent to profit."

After close examination of the undisputed facts involved in this case, we can only conclude that Reverend Falwell cannot demonstrate that Lamparello "had a bad faith intent to profit from using the [www.fallwell.com] domain name." Lamparello clearly employed www.fallwell.com simply to criticize Reverend Falwell's views. Factor IV of the ACPA counsels against finding a bad faith intent to profit in such circumstances because "use of a domain name for purposes of ... comment, [and] criticism," constitutes a "bona fide noncommercial or fair use" under the statute.[7] That Lamparello provided a link to an Amazon.com webpage selling a book he favored does not diminish the communicative function of his website. The use of a domain name to engage in criticism or commentary "even where done for profit" does not alone evidence a bad faith intent to profit, H.R. Rep. No. 106-412, and Lamparello did not even stand to gain financially from sales of the book at Amazon.com. Thus factor IV weighs heavily in favor of finding Lamparello lacked a bad faith intent to profit from the use of the domain name.

Equally important, Lamparello has not engaged in the type of conduct described in the statutory factors as typifying the bad faith intent to profit essential to a successful cybersquatting claim. First, we have already held that Lamparello's domain name does not create a likelihood of confusion as to source or affiliation. Accordingly, Lamparello has not engaged in the type of conduct—"creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site"—described as an indicator of a bad faith intent to profit in factor V of the statute.

Factors VI and VIII also counsel against finding a bad faith intent to profit here. Lamparello has made no attempt-or even indicated a willingness-"to transfer, sell, or otherwise assign the domain name to [Reverend Falwell] or any third party for financial gain." Similarly, Lamparello has not registered "multiple domain names"; rather, the record indicates he has registered only one. Thus, Lamparello's conduct is not of the suspect variety described in factors VI and VIII of the Act.

Notably, the case at hand differs markedly from those in which the courts have found a bad faith intent to profit from domain names used for websites engaged in political commentary or parody. For example, in *PETA* we found the registrant of www.peta.org engaged in cybersquatting because www.peta.org was one of *fifty* to *sixty* domain names Doughney had registered and because Doughney had evidenced a clear intent to sell www.peta.org to PETA, stating that PETA should try to "'settle' with him and 'make him an offer.'" Similarly, in Coca-Cola Co. v. Purdy, 382 F.3d 774 (8th Cir. 2004), the Eighth Circuit found an anti-abortion activist who had registered domain names incorporating famous marks such as "Washington Post" liable for cybersquatting because he had registered almost *seventy* domain names, had offered to stop using

[7] We note that factor IV does not protect a faux noncommercial site, that is, a noncommercial site created by the registrant for the sole purpose of avoiding liability under the FTDA, which exempts noncommercial uses of marks, or under the ACPA. As explained by the Senate Report discussing the ACPA, an individual cannot avoid liability for registering and attempting to sell a hundred domain names incorporating famous marks by posting noncommercial content at those domain names. But Lamparello's sole purpose for registering www.fallwell.com was to criticize Reverend Falwell, and this noncommercial use was not a ruse to avoid liability. Therefore, factor IV indicates that Lamparello did not have a bad faith intent to profit.

the Washington Post mark if the newspaper published an opinion piece by him on its editorial page, and posted content that created a likelihood of confusion as to whether the famous markholders sponsored the anti-abortion sites and "ha[d] taken positions on hotly contested issues." In contrast, Lamparello did not register multiple domain names, he did not offer to transfer them for valuable consideration, and he did not create a likelihood of confusion.

Instead, Lamparello, like the plaintiffs in two cases recently decided by the Fifth and Sixth Circuits, created a gripe site. Both courts expressly refused to find that gripe sites located at domain names nearly identical to the marks at issue violated the ACPA. In TMI, Inc. v. Maxwell, 368 F.3d 433, 434-35 (5th Cir. 2004), Joseph Maxwell, a customer of homebuilder TMI, registered the domain name "www.trendmakerhome.com," which differed by only one letter from TMI's mark, TrendMaker Homes, and its domain name, "www.trendmakerhomes.com." Maxwell used the site to complain about his experience with TMI and to list the name of a contractor whose work pleased him. After his registration expired, Maxwell registered "www.trendmakerhome.info." TMI then sued, alleging cybersquatting. The Fifth Circuit reversed the district court's finding that Maxwell violated the ACPA, reasoning that his site was noncommercial and designed only "to inform potential customers about a negative experience with the company."

Similarly, in *Lucas Nursery & Landscaping*, a customer of Lucas Nursery registered the domain name "www.lucasnursery.com" and posted her dissatisfaction with the company's landscaping services. Because the registrant, Grosse, like Lamparello, registered a single domain name, the Sixth Circuit concluded that her conduct did not constitute that which Congress intended to proscribe—i.e., the registration of multiple domain names. Noting that Grosse's gripe site did not create any confusion as to sponsorship and that she had never attempted to sell the domain name to the markholder, the court found that Grosse's conduct was not actionable under the ACPA. The court explained: "One of the ACPA's main objectives is the protection of consumers from slick internet peddlers who trade on the names and reputations of established brands. The practice of informing fellow consumers of one's experience with a particular service provider is surely not inconsistent with this ideal."

Like Maxwell and Grosse before him, Lamparello has not evidenced a bad faith intent to profit under the ACPA. To the contrary, he has used www.fallwell.com to engage in the type of "comment[ ][and] criticism" that Congress specifically stated militates against a finding of bad faith intent to profit. And he has neither registered multiple domain names nor attempted to transfer www.fallwell.com for valuable consideration. We agree with the Fifth and Sixth Circuits that, given these circumstances, the use of a mark in a domain name for a gripe site criticizing the markholder does not constitute cybersquatting.

IV.

For the foregoing reasons, Lamparello, rather than Reverend Falwell, is entitled to summary judgment on all counts. Accordingly, the judgment of the district court is reversed and the case is remanded for entry of judgment for Lamparello.

Prometek Industries, Ltd. v. Equitrac Corp., 300 F.3d 808 (7th Cir. 2002).
Williams, Circuit Judge.

This appeal concerns the propriety of a preliminary injunction in which one competitor, Prometek, prevailed against another, Equitrac. The preliminary injunction was issued without a hearing and Equitrac had to place language on its web page to remedy violations of the Lanham Act. Equitrac now appeals that order and because the district court did not abuse its discretion, we affirm.

I. BACKGROUND

Prometek and Equitrac are competitors in selling cost-recovery equipment. Equitrac's marketing department advised its web designer that certain words and phrases should be used as metatags for Equitrac's website.[1] In response, the web designer placed the term "Copitrack" in the contents of Equitrac's website as a metatag. Equitrac used the term as a metatag because it provides maintenance and service on Copitrak equipment, a product used in the cost-recovery business.[2] Prometek holds the trademark for Copitrak, and once it learned of Equitrac's use of the term Copitrack in the metatag, it brought suit. After learning of Prometek's suit, Equitrac contacted all of the search engines known to it and requested that they remove any link between the term Copitrack and Equitrac's website. Equitrac also removed the Copitrack metatag from its website.

Not satisfied with Equitrac's remedial measures, Prometek sought a preliminary injunction preventing Equitrac from using the term Copitrack in its website. After receiving materials submitted by both parties, the district court granted Prometek's motion for preliminary injunction. Under the terms of the injunction, Equitrac was directed to place language on its web page informing consumers that any link between its website and Copitrack was in error:

> If you were directed to this site through the term "Copitrack," that is in error as there is no affiliation between Equitrac and that term. The mark "Copitrak" is a registered trademark of Prometek Industries, Ltd., which can be found at www.prometek.com or www.copitrak.com.

Equitrac appeals the issuance of the injunction, arguing that the ordered language will not only inform consumers of its competitor, Prometek, but will encourage people to go to Prometek's website. Prometek counters that without this language, Equitrac will continue to benefit, to Prometek's detriment, from consumer internet searches containing the word Copitrack. We conclude that the district court was correct in finding Prometek would suffer a greater harm than Equitrac if corrective measures were not taken, and we affirm the grant of the preliminary injunction.

---

[1] [Quoting *Brookfield* for this definition:] Metatags are HTML [HyperText Markup Language] code intended to describe the contents of the web site. There are different types of metatags, but those of principal concern to us are the "description" and "keyword" metatags. The description metatags are intended to describe the web site; the keyword metatags, at least in theory, contain keywords relating to the contents of the web site. The more often a term appears in the metatags and in the text of the web page, the more likely it is that the web page will be "hit" in a search for that keyword and the higher on the list of "hits" the web page will appear.

[2] The parties agree that Equitrac meant to use the term "Copitrak" as its metatag rather than "Copitrack."

II. ANALYSIS…

A. The District Court Was Correct in Granting the Injunction

1. Likelihood of success on the merits

Equitrac argues that because there was no likelihood of success on the merits of Prometek's Lanham Act claim, the district court erred in granting the preliminary injunction. In order to prevail under the Lanham Act, 15 U.S.C. § 1125(a), Prometek must establish that Copitrak is a protectable trademark and that Equitrac's use of the term is likely to cause confusion among consumers. Preregistration of Prometek's Copitrak trademark is prima facie evidence of the mark's validity, which Equitrac does not dispute. Therefore, we turn to the issue of whether consumers would be confused by Equitrac's use of Copitrak as a metatag.

In assessing the likelihood of consumer confusion, we consider: (1) the similarity between the marks in appearance and suggestion, (2) the similarity of the products, (3) the area and manner of concurrent use of the products, (4) the degree of care likely to be exercised by consumers, (5) the strength of the plaintiff's marks, (6) any evidence of actual confusion, and (7) the defendant's intent to palm off its goods as those of the plaintiff's. None of these factors are dispositive and the proper weight given to each will vary in each case. However, the similarity of the marks, the defendant's intent, and evidence of actual confusion are of particular importance.

Given these factors, it is clear that Prometek has a fair likelihood of succeeding on the merits of its Lanham Act claim. Although Prometek has not provided us with evidence regarding the strength of its Copitrak mark or evidence of any actual consumer confusion, the other factors weigh in its favor. First, not only are the marks Copitrack and Copitrak similar, Equitrac admits that it meant to use the correct spelling of Copitrak in its metatag. Second, Equitrac's use of Copitrack refers to Prometek's registered trademark, Copitrak. Additionally, Equitrac and Prometek are direct competitors in the cost-recovery and cost-control equipment and services market. Most importantly, for purposes of this case, however, is the degree of care to be exercised by consumers.

Although Equitrac claims that it did not intend to mislead consumers with respect to Copitrak, the fact remains that there is a strong likelihood of consumer confusion as a result of its use of the Copitrack metatag. The degree of care exercised by consumers could lead to initial interest confusion. Initial interest confusion, which is actionable under the Lanham Act, occurs when a customer is lured to a product by the similarity of the mark, even if the customer realizes the true source of the goods before the sale is consummated.

The Ninth Circuit has dealt with initial interest confusion for websites and metatags and held that placing a competitor's trademark in a metatag creates a likelihood of confusion. In *Brookfield Communications*, the court found that although consumers are not confused when they reach a competitor's website, there is nevertheless initial interest confusion. This is true in this case, because by Equitrac's placing the term Copitrack in its metatag, consumers are diverted to its website and Equitrac reaps the goodwill Prometek developed in the Copitrak mark. That consumers who are misled to Equitrac's website are only briefly confused is of little or no

consequence. In fact, “that confusion as to the source of a product or service is eventually dispelled does not eliminate the trademark infringement which has already occurred.” What is important is not the duration of the confusion, it is the misappropriation of Prometek’s goodwill. Equitrac cannot unring the bell. As the court in *Brookfield* explained, “[u]sing another’s trademark in one’s metatags is much like posting a sign with another’s trademark in front of one’s store.” Customers believing they are entering the first store rather than the second are still likely to mill around before they leave. The same theory is true for websites. Consumers who are directed to Equitrac’s webpage are likely to learn more about Equitrac and its products before beginning a new search for Prometek and Copitrak. Therefore, given the likelihood of initial consumer confusion, the district court was correct in finding Prometek could succeed on the merits.

2. No adequate remedy at law

A plaintiff seeking a preliminary injunction must also prove that it has no adequate remedy at law and as a result, will suffer irreparable harm if the injunction is not issued. Furthermore, it is well settled that injuries arising from Lanham Act violations are presumed to be irreparable, even if the plaintiff fails to demonstrate a business loss.

As has been discussed, Prometek has suffered injury to its consumer goodwill through Equitrac’s use of Copitrack as a metatag and would have continued to suffer in the absence of an injunction. This damage would have constituted irreparable harm for which Prometek had no adequate remedy. Because of the difficulty in assessing the damages associated with a loss of goodwill, the district court was correct in finding that Prometek lacked an adequate remedy at law.

3. Balancing of the harms

The final factor we must consider is the balance of harms—the irreparable harm Equitrac will suffer if the injunction is enforced weighed against the irreparable harm Prometek will suffer if it is not. We must also consider the effect the injunction will have on the public. We review a district court’s balancing of the harms for an abuse of discretion.

In finding that the harm to Prometek as a result of denying the injunction outweighed the harm to Equitrac in granting it, the district court found, and we agree, that without the injunction, Equitrac would continue to attract consumers browsing the web by using Prometek’s trademark, thereby acquiring goodwill that belongs to Prometek. In response, Equitrac points out that even though it offers products for sale on its website, it has yet to consummate a sale by this means. Furthermore, Equitrac claims that “consumers of products and services provided by Equitrac and Prometek are sophisticated business people who are not likely to be confused between Equitrac and Copitrak and are not likely to buy based on a visit to a website.”

Although Equitrac claims that the language on its website is harmful because it alerts consumers to Prometek’s website, it has not provided any evidence of customers it has lost as a result of the remedial language. Indeed the remedial language on the website is more informative than it is harmful. Equitrac’s speculative argument that Prometek may gain a competitive advantage by inclusion of the remedial language is rejected. As to the public interest, because the injunction prevents consumer confusion in the marketplace, the public interest will be served as well. Accordingly, the strong likelihood of consumer confusion weighs strongly in favor of issuing the

injunction, and the district court did not abuse its discretion in finding this to be the case.

B. No evidentiary hearing was needed….
Equitrac claims that the court should not have issued the preliminary injunction without a hearing. Specifically, Equitrac argues that because the court failed to find, and did not receive evidence to contradict, Equitrac's position that it was entitled to advertise that it was capable of servicing Copitrak equipment, Promatek's motion for a preliminary injunction should have been denied. Equitrac's argument misses the point. What is relevant to the preliminary injunction is not that Equitrac may advertise that it is capable of servicing Copitrak. Equitrac is free to do so; it is also free to place comparison claims on its website, or include press releases involving the litigation between Equitrac and Promatek. *It is Equitrac's use of the term Copitrack in its metatag that is a prohibited practice because of its potential for customer confusion.* [Editor's note: regarding this italicized language, see below] Because Equitrac failed to demonstrate that its evidence would weaken Promatek's case, an evidentiary hearing was not necessary….

Promatek Industries, Ltd. v. Equitrac Corp., October 18, 2002 Amendment

The slip opinion of this Court issued on 8/13/02 is hereby amended as follows: On page 9, the second-to-last sentence of the first paragraph (beginning "It is Equitrac's use of the term...") should be removed and replaced with the following: "The problem here is not that Equitrac, which repairs Promatek products, used Promatek's trademark in its metatag, but that it used that trademark in a way calculated to deceive consumers into thinking that Equitrac was Promatek. Id." Immediately following the sentence to be inserted above, the following footnote should be inserted: "It is not the case that trademarks can never appear in metatags, but that they may only do so where a legitimate use of the trademark is being made."

AdWords Help (accessed July 9, 2010) (from http://adwords.google.com/support/aw/bin/answer.py?hl=en&answer=6118#content)

What is Google's AdWords and AdSense trademark policy?

Google recognizes the importance of trademarks. Our AdWords Terms and Conditions with advertisers prohibit intellectual property infringement by advertisers. Advertisers are responsible for the keywords they choose to generate advertisements and the text that they choose to use in those advertisements.

Google takes allegations of trademark infringement very seriously and, as a courtesy, we investigate matters raised by trademark owners. Trademarks are territorial and apply only to certain goods or services. Therefore, different parties can own the same mark in different countries or different industries. Accordingly, in processing complaints, Google will ask the trademark owner for information regarding where the mark is valid and for what goods or services. Please note the following about our complaint process:

- The trademark owner doesn't need to be a Google AdWords advertiser in order to send a complaint.
- Any such investigation will only affect ads served on or by Google.
- Google's trademark policy does not apply to search results. Our investigations only apply to sponsored links. For trademark concerns about websites that appear in Google search results, the trademark owner should contact the site owner directly.
- In the case of an AdSense for Domains trademark complaint, an investigation will affect only the participation of the domain name in question in our AdSense for Domains program.
- Because Google is not a third-party arbiter, we encourage trademark owners to resolve their disputes directly with the advertisers, particularly because the advertisers may have similar ads running via other advertising programs.

AdWords Trademark Policies in Sponsored Links

Below, you can find information on our trademark complaint procedure across different regions as well as on our advertiser authorization procedure.

I see an unauthorized ad using my trademark. What is Google's trademark policy?

Depending on the regions in which you have trademark rights, we may investigate the use of trademarks in ad text only or in ad text and keywords.

Please note the regions we will investigate ad text only. We will not disable keywords in response to a trademark complaint. Furthermore, our investigation will only affect ads served on or by Google.

Regions in which we investigate use in ad text only

In the U.S., we allow some ads to show with a trademark in ad text if the ad is from a reseller or from an informational site. However, if our investigation finds that the advertiser is using the trademark in the ad text in a manner which is competitive, critical, or negative, we will require the advertiser to remove the trademark and prevent them from using it in similar ad text in the future. Learn more about our U.S. trademark policy.

Outside the U.S., if our investigation finds that the advertiser is using the trademark in ad text, we will require the advertiser to remove the trademark and prevent them from using it in ad text in the future.

Google is dedicated to providing relevant advertising to our users, advertisers, and publishers alike. Accordingly, our trademark policy not to investigate the use of trademarks as keywords in the regions listed above aims to provide users with choices relevant to their keywords. At the same time, we investigate trademark violations in ad text, both as a courtesy to the trademark owner and to ensure that ads are clear to users.

In certain regions, we may investigate use of trademarks in ad text, in keywords, or in both ad text and keywords.

Regions in which we investigate use in both ad text and keywords

When we receive a complaint from a trademark owner, our review is limited to ensuring that the advertisements at issue are not using a term corresponding to the trademarked term in the ad text or as a keyword. If they are, we will require the advertiser to remove the trademarked term from the ad text or keyword list and will prevent the advertiser from using the trademarked term in the future. Any such investigation will only affect ads served on or by Google.

We do not take any action in situations where an advertisement is being triggered by non-trademarked terms even though the search query contains a trademarked term. This occurrence stems from the fact that Google allows advertisers to use a broad matching system to target their ads. For example, if an advertiser has selected the keyword “shoes,” that advertiser’s ad will appear when a user enters the word “shoes” as a search query, regardless of other search terms that may be used. So, the ad would show if the user entered any of the following search queries: “tennis shoes,” “red shoes,” or “Nike shoes.” This system eliminates the need for the advertiser to specify each of the myriad different search query combinations that are relevant to their ad.

AdWords Counterfeit Goods Complaint in Sponsored Links

A Google advertiser is selling counterfeit goods. What is Google’s Counterfeit Goods policy?

Google AdWords prohibits the sale or promotion of counterfeit goods. Counterfeit goods contain a trademark or logo that is identical to or substantially indistinguishable from the trademark of another. They mimic the brand features of the product in an attempt to pass themselves off as a genuine product of the brand owner, or they promote the goods as faux, replicas, imitations or clones of the original product.

• AdWords Counterfeit vs. Trademark Policy:
Our counterfeit policy concerns the actual goods promoted on the site in question, whereas our trademark policy concerns use of the trademark in the ad text or keywords (in certain circumstances) in the ad itself.

• AdWords Counterfeit vs. DMCA/Copyright/Pirated Goods:
Counterfeiters mimic the trademark brand features, rather than copying the product itself (software, books, artwork, movies, etc.).

We will investigate all reasonable complaints; our actions may include disapproving or disabling ads and/or terminating advertisers. Any such investigation and action will only affect ads served on or by Google.

Please note that, upon request and approval, a complainant's contact details may be forwarded to the affected advertiser(s).

If you have concerns about the sale of counterfeit goods in AdWords ads, please file a complaint.

AdSense for Domains Trademark Policy

A parked domain is serving AdSense ads, and the domain name is using my trademark or variation thereof. What is Google's AdSense for Domains trademark policy?

Google provides an ad serving program via our AdSense for Domains service, wherein domain registrars can display ads on their inactive domains. If you are unsure what a parked domain is, please review this page before submitting a complaint.

If you have concerns about the use of your trademark as a parked domain name, file an AdSense for Domains trademark complaint. Once Google receives all of the required information from the trademark owner, the claim will be investigated, and appropriate action will be taken.

Hearts on Fire Company, LLC v. Blue Nile, Inc., 603 F. Supp. 2d 274 (D. Mass. 2009).
Gertner, District Judge.

This case raises complex allegations of trademark infringement on the internet—through the use of trademarks in search engines, in sponsored links, and on commercial websites. The Plaintiff, Hearts on Fire Co., LLC ("Hearts on Fire"), principally claims that one of its competitors, Blue Nile, Inc. ("Blue Nile"), committed trademark infringement when it used the Plaintiff's trademark as a keyword to trigger search engine advertisements known as "sponsored links." While sponsored linking is a common form of internet advertising, the use of a competitor's trademark to trigger these links has generated both litigation and academic debate.

The Complaint encompasses three different uses of the Plaintiff's mark by Blue Nile: (1) the Defendant's purchase of the trademark as a search engine keyword, which displayed a sponsored link directing the computer user to Blue Nile's website whenever the phrase "hearts on fire" was entered as a search-term, (2) the display of trademarked text in the Blue Nile advertisement attached to the sponsored link, and (3) the search results list generated within the Blue Nile website when the computer user searches there for the phrase "hearts on fire." Together, the Plaintiff argues, these uses constitute a course of conduct likely to confuse internet shoppers, improperly diverting them to its competitor's website.

The Defendant has filed a Motion to Dismiss. Significantly, the Defendant's present motion is not directed toward Plaintiff's allegation that the trademark "hearts on fire" appeared alongside Defendant's sponsored link. Blue Nile agrees that this allegation, if true, amounts to infringement. Rather, Blue Nile asks this Court to dismiss the Plaintiff's allegation that the Defendant's use of the trademark to trigger the sponsored link constitutes infringement under Section 32(a) of the Lanham Act, 15 U.S.C. § 1114. Likewise, the Defendant argues that Plaintiff's third theory is unavailing, because Blue Nile does not use the "hearts on fire" trademark on its own website.

For the reasons below, the Court finds that Blue Nile's adoption of the Plaintiff's trademark as a search engine keyword constitutes a "use" within the meaning of the Lanham Act. To be sure, this use is not, by itself, enough to prove infringement. If the Plaintiff can show that the resulting sponsored links and the content of the Blue Nile website likely led to consumer confusion, Blue Nile's purchase of the search term would meet the requirements of the Act. Accordingly, Blue Nile's Motion to Dismiss is **DENIED**.

I. BACKGROUND

The Plaintiff sells trademarked diamonds and jewelry to authorized retailers, many of whom resell these diamonds online. "Hearts on Fire" is a registered trademark of the Plaintiff, and the name of the Plaintiff's diamond company. The Plaintiff does not sell diamonds directly to the public, though it does "provide services relating to the sale of jewelry," including a public website that promotes the trademarked jewelry and directs customers to authorized dealers of the trademarked diamonds. The Plaintiff considers itself a "recognized worldwide industry leader," which has used the trademark "Hearts on Fire" to promote its diamonds since as early as 1996.

The Defendant, Blue Nile, operates an online diamond and jewelry retail store where consumers can purchase diamonds. Importantly, the Defendant is not an authorized dealer of Hearts on Fire diamonds and consumers cannot buy the Plaintiff's trademarked diamonds at the Defendant's website.

The mechanisms of the alleged infringement, which is based upon keyword purchasing and the display of search engine sponsored links, warrant some description. When a consumer wants to search the internet for information, she or he often begins at a search engine, such as Google or Yahoo. Once there, the computer user types words or phrases into a search box on the search engine website. The search engine then generates a list of web addresses, called a "search results list," that may be relevant to the computer user's interests based on the searched-for word or phrase. Search engines use complex algorithms to search their databases and determine which web addresses will appear in the search results list. These algorithms generally rank the web addresses according to relevancy, using factors such as whether the search terms appear on the webpage and whether previous computer users using that search term have decided to click on the link to the web address.

In addition to search results based on relevancy, many search engines also display so-called "sponsored links" on their results page. These sponsored links are a form of advertising, by which the search engine permits a company to purchase a keyword or phrase which triggers the paid advertisement. Specifically, when a computer user enters a search that includes the purchased keyword, a link to the website of the company that purchased the keyword, together with a small advertisement, appears near the top of the results list displayed. This listing is usually demarcated, quite accurately, as a "sponsored link." All in all, purchasing a keyword allows a company to circumvent the search engine's usual relevancy factors and prominently display its sponsored link to internet users.

In this case, the Plaintiff alleges that the Defendant paid a search engine, www.webcrawler.com, to display a sponsored link with the web address of the Defendant's website when a computer user searched for the phrase "hearts on fire." The text of the sponsored link, which included the Plaintiff's trademark, reads as follows:

> Ideal Cut Diamonds at Blue Nile
> Find hearts on fire diamonds at Forbes Favorite Online Jeweler.
> Sponsored by: www.bluenile.com.

The Plaintiff also alleges that the Defendant has used the "hearts on fire" keyword to trigger Blue Nile sponsored links that do not include the trademark in their text. In either case, if the internet user clicks the sponsored link and proceeds to the Defendant's web address, www.bluenile.com, the Blue Nile website contains an internal search engine that exclusively searches web pages within the Defendant's website. If the computer user then types the trademarked phrase into the Defendant's search box, a list of search results containing the individual words of the trademark are displayed—i.e., a list of webpages with the words "hearts" or "on fire"—albeit none of these results containing the exact trademarked phrase.

The Plaintiff alleges that these uses of its mark, either separately or together, constitute trademark infringement under Section 32(a) of the Lanham Act, 15 U.S.C. § 1114, unfair competition under Section 43(a) of the Lanham Act, 15 U.S.C. § 1125(a), unfair competition at common law, and unfair and deceptive practices under M.G.L. ch. 93A. Plaintiff is harmed because Defendant's use of the "hearts on fire" trademark confuses consumers, diverting potential internet customers from their original intent to buy the Plaintiff's diamonds and directing them instead to the Defendant's website. Whether this diversion—achieved through the purchase of sponsored links triggered by the trademarked phrase—constitutes trademark infringement is the central issue here….

III. DISCUSSION

The Defendant has filed a partial motion to dismiss, seeking to eliminate the first and third theories of trademark violation that the Plaintiff pursues, namely the Defendant's purchase of the "hearts on fire" trademark as a keyword to trigger sponsored links, and the results when "hearts on fire" is entered into the Defendant's internal search engine. As described above, the Defendant has not challenged the allegation that the sponsored link's display of the exact trademarked phrase as part of the accompanying advertisement, if proved, would amount to a trademark violation.

A. The Lanham Act

The Lanham Act serves two basic purposes: foremost, preventing the use of similar or identical marks in a way that confuses the public about the actual source of the goods and services; and second, the protection of the goodwill that companies have built up in their trademarks. To establish liability, the Plaintiff must ultimately prove that (1) it owns and uses the "Hearts on Fire" trademark; (2) the Defendant used the trademark without the Plaintiff's permission; and (3) the Defendant's use was likely to confuse consumers, thereby causing the Plaintiff harm. While the Plaintiff has clearly pleaded facts sufficient to show that it owns the trademark, the parties debate whether the keyword purchase constitutes a "use" under the Lanham Act and what standard of confusion the Plaintiff must meet.

B. The "Use" Requirement

As an initial matter, this Court must resolve whether the purchase of a trademarked keyword to trigger a sponsored link constitutes a "use" of that trademark, as the first prong of the Lanham Act requires. The circuits have split on the issue; the First Circuit has not yet squarely decided such a case.[4]

[4] The First Circuit recently considered a similar, though not identical, case of internet trademark infringement, where the defendant company had allegedly embedded in its website invisible HTML code, or "meta-tags", containing its competitor's trademark, in order to attract increased search engine traffic. See Venture Tape Corp. v. McGills Glass Warehouse, 540 F.3d 56 (1st Cir. 2008). In its analysis, however, the First Circuit focused exclusively on the second prong of the Lanham Act, the likelihood of consumer confusion. It assumed, without deciding, that the defendant's embedding of the trademark in invisible meta-tags qualified as a "use" under the first prong of the Lanham Act, despite the fact that consumers do not see such embedded marks. With this question still unresolved, this Court is obliged to conduct an independent inquiry into whether the "use" requirement has been met here, reaching a conclusion consistent with the First Circuit's assumption in Venture Tape.

At present, the Second Circuit stands alone in holding that the purchase of a competitor's trademark to trigger internet advertising does not constitute a use for the purposes of the Lanham Act. The pivotal case, 1-800 Contacts, Inc. v. WhenU.Com, Inc., did not involve sponsored links as here, but rather a different form of internet advertising known as "pop-up ads." 414 F.3d 400 (2d Cir. 2005). In *1-800 Contacts*, Vision Direct, a phone directory company and competitor of 1-800 Contacts, Inc., paid WhenU.com to display a pop-up advertisement on a computer user's screen whenever he or she entered "www.1800contacts.com" as a web address. The pop-up ad created a new window with Vision Direct's advertisement, temporarily blocking the 1800contacts.com website from view.

Crucially, the Second Circuit held that the www.1800contacts.com web address was "similar, but not identical" to the company's protected trademark, "1-800 CONTACTS." Likewise, because the pop-up advertisement did not actually display the 1-800 Contacts trademark anywhere in its text, the Second Circuit held that there was no "use" of the trademark within the meaning of the Lanham Act. In this view, only the web address—not the trademark itself—was used to trigger the Vision Direct advertisement, and even that use was confined to an internal software directory never seen by the internet user. As such, the Second Circuit found that the pop-up ad did not rely on any use of the trademark itself, nor did it create any possibility of "visual confusion" with 1-800 Contacts' mark.

While *1-800 Contacts* carefully distinguished the pop-up advertisement context from the keyword context, lower courts in the Second Circuit have gone further. They have applied that same reasoning to keyword cases, holding that a company's purchase of a competitor's trademark to trigger sponsored links does not qualify as a "use." Whether such an extension of the Second Circuit's reasoning in *1-800 Contacts*, a pop-up ad case, is warranted in a sponsored-link case like this one is questionable.

Indeed, outside of the Second Circuit, other circuits agree that the purchase of trademarks to trigger banner advertisements on a search results page is a "use" under the Lanham Act.[6] See Playboy Enterprises, Inc. v. Netscape Commc'ns Corp., 354 F.3d 1020 (9th Cir. 2004); Australian Gold, Inc. v. Hatfield, 436 F.3d 1228 (10th Cir. 2006). District courts have followed suit when applying these decisions to the purchase of trademarked keywords to trigger sponsored links.

Rather than relying only on the Act's definitions section as the Second Circuit has done, these courts often look also to its civil remedies provision, which defines "use" more broadly. In particular, the civil remedies provision penalizes the "use in commerce" of "any reproduction, counterfeit, copy, or colorable imitation of a registered mark *in connection with* the sale, offering for sale, distribution, or advertising of any goods or services." 15 U.S.C. § 1114 (emphasis added). The purchase of a competitor's trademark to trigger search-engine advertising is precisely such a use in commerce, even if the trademark is never affixed to the goods themselves. In effect, one company has relied on its competitor's trademark to place advertisements for its own products in front of consumers searching for that exact mark. The Lanham Act's use

[6] Unlike a sponsored link, banner advertisements are not displayed as part of a search results list, but instead often occupy the margins of a webpage.

requirement is not so narrow or cramped that it would fail to treat this conduct as a "use in commerce."

Even the Act's definitions section, which pre-dates the advent of internet commerce and advertising, treats as a "use in commerce" any use of the trademark on "displays associated" with the goods offered for sale. On the facts of this case, by contrast to *1-800 Contacts*, a computer user's search for the trademarked phrase necessarily involves a display of that trademark as part of the search-results list. For instance, if a computer user searches for the "hearts on fire" trademark at www.webcrawler.com, the text "Web search results for 'hearts on fire'" is prominently displayed above the search results, including the sponsored links. Indeed, this display is exactly what the Defendant paid for: the association of Blue Nile's sponsored link with the searched-for trademark.

In light of the Lanham Act's language and the broader purposes of the trademark statute, there is little question that the purchase of a trademarked keyword to trigger sponsored links constitutes a "use" within the meaning of the Lanham Act.

C. Likelihood of Confusion

Although Blue Nile's alleged keyword purchase fulfills the "use" prong of the Lanham Act, it is only one element of trademark infringement and does not constitute a violation in and of itself. The Plaintiff still must prove a likelihood of confusion, which generally involves a far more fact-specific inquiry: whether "the allegedly infringing conduct carries with it a likelihood of confounding an appreciable number of reasonably prudent purchasers exercising ordinary care."

At this stage in the case, there is no suggestion that diverted consumers inadvertently believed they were purchasing Hearts on Fire diamonds at Blue Nile's website. No diamonds appearing on the website purport to be Hearts on Fire diamonds. Rather, Plaintiff relies on allegations of pre-sale confusion to support its infringement claim. Most relevant in light of this partial Motion to Dismiss is Plaintiff's argument that even those sponsored links which did *not* display its trademark likely confused consumers. That is, the simple fact an internet user entered a search for its trademarked diamonds and, in response, received a link to Blue Nile's diamond retail website was enough to confuse the online shopper—even if the sponsored link did not use the trademark in its text at all. This sequence, according to the Plaintiff, was actionable because it sparked an initial interest in Blue Nile's products, leading its potential customers astray in violation of trademark protections.

1. Initial Interest Confusion

The Plaintiff argues that the likelihood of confusion prong can be fulfilled in this case by resort to a trademark doctrine called "initial interest confusion." A somewhat ill-defined concept, initial interest confusion refers to a type of pre-sale confusion that has not been fully explored or addressed by the First Circuit. Generally speaking, pre-sale confusion refers to a potential purchaser's temporary confusion about the actual source of goods or services under consideration, even where that confusion is resolved by the actual moment of sale. There is no question that this type of confusion falls squarely within the scope of trademark violations contemplated by the Lanham Act. In fact, the 1962 amendments to the Act explicitly brought

pre-sale confusion within the ambit of trademark protections. Lanham Act, § 32(1)(a), as amended, 15 U.S.C. § 1114(1)(a); Oct. 9, 1962, Pub.L. 87-772, § 17, 76 Stat. 773 (removing the term "purchasers" to expand trademark protection to situations involving pre-sale as well as point-of-sale and post-sale confusion). Obviously, bringing pre-sale confusion within the Act did not lighten plaintiffs' burden of showing confusion. They still must show that "an appreciable number of reasonably prudent consumers" would likely be confused about the source of the marketed goods or services at some point during the pre-sale process.

Initial interest confusion targets one specific type of pre-sale confusion: It involves confusion at the very earliest stage—not with respect to the source of specific goods or services under consideration, but during the process of searching and canvassing for a particular product. The classic example is where a consumer sets out in search of one trademarked good, but is then sidetracked en route to his or her original destination by a competitor's advertisement or offering. He or she is never confused as to the source or origin of the product he eventually purchases, but he may have arrived there through either misdirection or mere redirection. In effect, initial interest confusion involves the diversion of the consumer's attention from one trademarked good to a competing good, even if he is not confused about the source of the products he ultimately considers or buys.

Early "initial interest confusion" cases in the bricks-and-mortar world involved the use of similar trademarks that might mislead a consumer searching for a particular product. In these cases, which appear relatively rare, the consumer did not buy the item believing that it was the trademarked good. Rather, he was confused at an early point in the pre-sale process. See Grotrian, Helfferich, Schulz, Th. Steinweg Nachf. v. Steinway & Sons, 523 F.2d 1331, 1342 (2d Cir. 1975) (piano company using similar name to trademarked company misled consumers); Mobil Oil Corp. v. Pegasus Petroleum Corp., 818 F.2d 254 (2d Cir. 1987) (oil company with name invoking plaintiff's trademarked logo confused oil traders into investing a considerable amount of time and effort into pre-sale negotiations with the defendant).[8]

As trademark doctrine has evolved, particularly in the internet context, initial interest confusion has been invoked in a widening range of scenarios. One was illustrated by the Ninth Circuit in Brookfield Communications Inc. v. West Coast Entertainment Corp., 174 F.3d 1036, 1062 (9th Cir. 1999). There, the court compared invisible embedding of the plaintiff's trademark in the defendant's webpage (i.e., meta-tags) to a misleading billboard:

> Suppose West Coast's competitor (let's call it 'Blockbuster') puts up a billboard on a highway reading—'West Coast Video: 2 miles ahead at Exit 7'—where West Coast is really located at Exit 8 but Blockbuster is located at Exit 7. Customers looking for West Coast's store will pull off at Exit 7 and drive around looking for it. Unable to locate West Coast, but seeing the Blockbuster store right by the highway entrance, they may simply rent there.

[8] As several commentators note, "'Initial interest confusion' as originally conceived did not reflect a new doctrine; rather, it was a simple recognition that competition-distorting confusion can occur at times other than the point of sale." Stacey Dogan and Mark Lemley, Trademarks and Consumer Search Costs on the Internet; 41 Hous. L.Rev. 777, 814 (2004).

In this scenario, the trademark is employed not to fool the consumer about his eventual purchase, but to lead him astray on false pretenses and into the arms of a competitor. The Ninth Circuit held that this use of a competitor's trademark in a meta-tag constituted infringement under an initial interest theory; a number of other courts have followed suit. Using a competitor's trademark to lure a consumer off the highway and into one's store, in this view, is little different from confusing the consumer when he steps through the door.

As a hypothetical, the Ninth Circuit's billboard example may state a perfectly plausible case of trademark infringement. One company has used a direct display of its competitor's mark to confuse consumers in a fashion that is costly, sustained, and not easily reversed. Whether the mark is used on the competing goods themselves or on a sign pointing the way makes little difference in the trademark calculus. The culprit has misappropriated the goodwill embodied by the protected mark and has increased consumer search costs through misdirection. But rarely are cases so clear as the Ninth Circuit's billboard—particularly on the internet—and certainly not this one.

Indeed, sponsored link advertising invites a second type of comparison: Initial interest confusion, for example, has been invoked in circumstances where one company "piggybacks" on its competitor's trademark, rewarding his search for one particular product with a choice among several similar items. Infringement is not nearly so obvious from this vantage point. Rather than a misleading billboard, this analogy is more akin to a menu—one that offers a variety of distinct products, all keyed to the consumer's initial search. Sponsored linking may achieve precisely this result, depending on the specific product search and its context. When a consumer searches for a trademarked item, she receives a search results list that includes links to both the trademarked product's website and a competitor's website. Where the distinction between these vendors is clear, she now has a simple choice between products, each of which is as easily accessible as the next. If the consumer ultimately selects a competitor's product, she has been diverted to a more attractive offer but she has not been confused or misled.[9] While she may have gotten to the search-results list via the trademarked name, once there, the advertised products are easily distinguished.

In much the same way, keyword purchasing may, in many cases, be analogized to a drug store that "typically places its own store-brand generic products next to the trademarked products they emulate in order to induce a customer who has specifically sought out the trademarked product to consider the store's less-expensive alternative." 1-800 Contacts, Inc. v. WhenU.Com, Inc., 414 F.3d 400, 411 (2d Cir. 2005). The generic product capitalizes on the recognizable brand name but the consumer benefits by being offered a lower-cost product. At no point is the consumer confused about the alternatives presented to her. The goodwill invested in the protected mark remains undisturbed while the consumer reaps the benefit of competing goods. Trademark infringement would seem to be unsupportable in this scenario. Mere diversion, without any hint of confusion, is not enough.

[9] Consider, for instance, if Pepsi were to purchase sponsored links to its website triggered by an internet user's search for the "Coca-Cola" trademark. Coca-Cola would have difficulty suing Pepsi for infringement on an initial interest theory because these two products are widely recognized as competitors and, accordingly, the likelihood of consumer confusion is exceedingly small.

2. Balancing Consumer Confusion and Consumer Search Costs

To be sure, the sponsored links appearing on a search-results page will not always be a menu of readily distinguished alternatives. With the intense competition for internet users' attention and mouse-clicks, online merchants may well be tempted to blur these distinctions, hoping to create and capitalize on initial consumer confusion. Such conduct undoubtedly begins to sound in trademark infringement. Thus, where a plaintiff has plausibly alleged some consumer confusion, even at an initial stage of his product search, the question is a far closer one. The First Circuit does view *pre-sale* confusion, generally, as actionable—as the amended statute allows and as most circuits have since found. But the First Circuit has never addressed initial interest confusion. See Hasbro, Inc. v. Clue Computing, Inc., 232 F.3d 1, 2 (1st Cir. 2000) (crediting the lower court for its "refusal to enter the 'initial interest confusion' thicket"); EMC Corp. v. Hewlett-Packard Co., 59 F. Supp. 2d 147, 150 (D.Mass. 1999) (concluding that the First Circuit had not squarely considered or taken a position on initial interest confusion); Beacon Mut. Ins. Co. v. OneBeacon Ins. Group, 290 F. Supp. 2d 241 (D.R.I. 2003) (collecting initial interest confusion cases), rev'd on other grounds, 376 F.3d 8 (1st Cir. 2004). But see Northern Light Tech. v. Northern Lights Club, 97 F. Supp. 2d 96, 113 (D. Mass. 2000) (finding initial interest confusion "not cognizable" under the First Circuit's trademark law), aff'd on other grounds, 236 F.3d 57 (1st Cir. 2001) (without discussion of initial interest confusion). Without First Circuit guidance, this Court is obliged to decide whether a plaintiff pleading initial interest confusion may state a claim for trademark infringement. Based on the twin goals of trademark protection, the Court concludes that initial interest confusion can support a claim under the Lanham Act—but only where the plaintiff has plausibly alleged that consumers were confused, and not simply diverted.

Many cases, including this one, will fall somewhere between the incarnations of so-called initial interest confusion discussed above—the misleading billboard or the choice-enhancing menu. The Court's task is to distinguish between them. As a preliminary matter, the Court agrees with the many scholars who find the deceptive billboard analogy often inapt in the internet context. Unlike the deceived shopper who is unlikely to get back on the highway, the internet consumer can easily click the 'back' button on her web browser and return almost instantly to the search results list to find the sought-after brand. Her added search costs, in other words, may often be very low while her comparative choice among products is greatly expanded.

The ease with which an internet shopper can reverse course counsels against over-expansive trademark protection, as any confusion may be extremely temporary and quickly remedied. The choice-enhancing properties of internet advertising should not be stifled on account of fleeting confusion among competing products. Trademark protections must ultimately accrue to the consumer's benefit.

The crucial question in these cases is one of degree: Whether the consumer is likely confused in some sustained fashion by the sponsored link and the defendant's website, or whether the link serves instead as a benign and even beneficial form of comparison shopping. The menu analogy described above—where the competing products are clearly distinguished—is not, in and of itself, truly a case of confusion at all, and therefore cannot support an infringement claim. In fact, in order for a plaintiff pleading initial interest confusion to prevail, that confusion must be more than momentary and more than a "mere possibility." As with any alleged trademark violation,

plaintiffs must show a genuine and "substantial" likelihood of confusion. The alleged confusion must be truly costly to the consumer.

This principle was implicit in the bricks-and-mortar cases that laid the groundwork for initial interest confusion as well as the Ninth Circuit's billboard analogy, which assumed that the deceived shopper, once diverted, would not get back on the highway. Where, as here, a plaintiff has alleged a plausible likelihood of confusion based on the overall context in which a consumer performs his internet search, see infra, he has stated a claim for trademark infringement and may proceed on an initial interest theory.

3. Blue Nile's Sponsored Links

In assessing the likelihood of confusion, the first question for the Court is, which of the two scenarios above apply to Blue Nile's sponsored links: Were consumers misdirected by the search results, like a misleading billboard, or simply offered a menu of distinct, competing products? And second, if consumers were potentially misdirected by Blue Nile's sponsored links, was that potential for confusion sufficient to state a claim for trademark infringement?

Before proceeding, it is useful to review what conduct is presently before the Court. The sponsored link identified by Hearts on Fire in its Complaint resembles the billboard hypothetical above because it involved a direct display of the "Hearts on Fire" trademark. Not even Blue Nile contests, at this stage of the litigation, that this allegation states a claim for trademark infringement. The question is whether Blue Nile's use of the trademark as a keyword trigger for sponsored links whose text did not contain the plaintiff's trademark is actionable.

On the facts alleged in the Complaint, the Court finds that Hearts on Fire has stated a claim for trademark infringement, even where Blue Nile's sponsored links did not display the protected mark. In particular, the Plaintiff has offered sufficient allegations to support its claim that consumers were likely confused, and potentially misled, by Blue Nile's use of the trademark as a trigger for its sponsored links. While these advertisements may not have displayed the mark itself, the surrounding context supplies a sufficient basis to support allegations of consumer confusion at this early stage of the litigation.

Hearts on Fire is a diamond wholesaler, while Blue Nile is an internet diamond retailer; the two companies are not plain or obvious competitors. In fact, the Plaintiff sells its products online through authorized retailers who operate their own websites. A consumer who had just entered a search for Hearts on Fire diamonds might easily believe that the Defendant was one such authorized retailer when presented with Blue Nile's sponsored link, even if the accompanying text did not contain the trademarked phrase. This conclusion is perfectly commonsensical under the circumstances, even if search engines often return irrelevant results. Moreover, if the consumer clicked on the sponsored link thinking that he would find the sought-after diamonds at Blue Nile's website, Plaintiff alleges that on arrival nothing there would immediately alert him to his mistake. Whether this likely confusion was sufficiently sustained on all the facts for Plaintiff to prevail on its infringement claim is a question for summary judgment. For now, the Plaintiff has alleged enough.

Looking ahead, the First Circuit has identified eight criteria that a court should look to when determining whether a trademark use is likely to confuse an appreciable number of consumers: (1) the similarity of the marks; (2) the similarity of the goods; (3) the relationship between their channels of trade; (4) the relationship between their advertising; (5) the classes of their prospective purchasers; (6) any evidence of actual confusion of internet consumers; (7) the defendant's subjective intent in using the mark; and (8) the overall strength of the mark. Importantly, though "evidence of actual confusion is 'often deemed the best evidence of possible future confusion, proof of actual confusion is not essential to finding likelihood of confusion.'" Indeed, the First Circuit has acknowledged the difficulty of obtaining such evidence in the internet context. Thus, while proof of actual confusion is not required to show trademark infringement, the Plaintiff must still prove likely confusion based on inferences from the other seven factors.

In addition to these familiar factors, under the circumstances here, the likelihood of confusion will ultimately turn on what the consumer saw on the screen and reasonably believed, given the context. This content and context includes: (1) the overall mechanics of web-browsing and internet navigation, in which a consumer can easily reverse course; (2) the mechanics of the specific consumer search at issue; (3) the content of the search results webpage that was displayed, including the content of the sponsored link itself; (4) downstream content on the Defendant's linked website likely to compound any confusion; (5) the web-savvy and sophistication of the Plaintiff's potential customers; (6) the specific context of a consumer who has deliberately searched for trademarked diamonds only to find a sponsored link to a diamond retailer; and, in light of the foregoing factors, (7) the duration of any resulting confusion. This list is not exhaustive, but it identifies what the Court views as the most relevant elements to showing a likelihood of confusion in this case….

Tiffany Inc. v. eBay, Inc., 600 F.3d 93 (2d Cir. N.Y. 2010).
Sack, Circuit Judge.

eBay, Inc. ("eBay"), through its eponymous online marketplace, has revolutionized the online sale of goods, especially used goods. It has facilitated the buying and selling by hundreds of millions of people and entities, to their benefit and eBay's profit. But that marketplace is sometimes employed by users as a means to perpetrate fraud by selling counterfeit goods.

Plaintiffs Tiffany (NJ) Inc. and Tiffany and Company (together, "Tiffany") have created and cultivated a brand of jewelry bespeaking high-end quality and style. Based on Tiffany's concern that some use eBay's website to sell counterfeit Tiffany merchandise, Tiffany has instituted this action against eBay, asserting various causes of action—sounding in trademark infringement, trademark dilution and false advertising—arising from eBay's advertising and listing practices. For the reasons set forth below, we affirm the district court's judgment with respect to Tiffany's claims of trademark infringement and dilution but remand for further proceedings with respect to Tiffany's false advertising claim.

BACKGROUND…

eBay
eBay is the proprietor of www.ebay.com, an Internet-based marketplace that allows those who register with it to purchase goods from and sell goods to one another. It "connect[s] buyers and sellers and [ ] enable[s] transactions, which are carried out directly between eBay members." In its auction and listing services, it "provides the venue for the sale [of goods] and support for the transaction[s], [but] it does not itself sell the items" listed for sale on the site, nor does it ever take physical possession of them. Thus, "eBay generally does not know whether or when an item is delivered to the buyer."

eBay has been enormously successful. More than six million new listings are posted on its site daily. At any given time it contains some 100 million listings.

eBay generates revenue by charging sellers to use its listing services. For any listing, it charges an "insertion fee" based on the auction's starting price for the goods being sold and ranges from $0.20 to $4.80. For any completed sale, it charges a "final value fee" that ranges from 5.25% to 10% of the final sale price of the item. Sellers have the option of purchasing, at additional cost, features "to differentiate their listings, such as a border or bold-faced type."

eBay also generates revenue through a company named PayPal, which it owns and which allows users to process their purchases. PayPal deducts, as a fee for each transaction that it processes, 1.9% to 2.9% of the transaction amount, plus $0.30. This gives eBay an added incentive to increase both the volume and the price of the goods sold on its website.

Tiffany
Tiffany is a world-famous purveyor of, among other things, branded jewelry. Since 2000, all new Tiffany jewelry sold in the United States has been available exclusively through Tiffany's retail stores, catalogs, and website, and through its Corporate Sales Department. It does not use

liquidators, sell overstock merchandise, or put its goods on sale at discounted prices. It does not—nor can it, for that matter—control the "legitimate secondary market in authentic Tiffany silvery jewelry," i.e., the market for second-hand Tiffany wares. The record developed at trial "offere[d] little basis from which to discern the actual availability of authentic Tiffany silver jewelry in the secondary market."

Sometime before 2004, Tiffany became aware that counterfeit Tiffany merchandise was being sold on eBay's site. Prior to and during the course of this litigation, Tiffany conducted two surveys known as "Buying Programs," one in 2004 and another in 2005, in an attempt to assess the extent of this practice. Under those programs, Tiffany bought various items on eBay and then inspected and evaluated them to determine how many were counterfeit. Tiffany found that 73.1% of the purported Tiffany goods purchased in the 2004 Buying Program and 75.5% of those purchased in the 2005 Buying Program were counterfeit. The district court concluded, however, that the Buying Programs were "methodologically flawed and of questionable value," and "provide[d] limited evidence as to the total percentage of counterfeit goods available on eBay at any given time." The court nonetheless decided that during the period in which the Buying Programs were in effect, a "significant portion of the 'Tiffany' sterling silver jewelry listed on the eBay website ... was counterfeit," and that eBay knew "that some portion of the Tiffany goods sold on its website might be counterfeit." The court found, however, that "a substantial number of authentic Tiffany goods are [also] sold on eBay."

Reducing or eliminating the sale of all second-hand Tiffany goods, including genuine Tiffany pieces, through eBay's website would benefit Tiffany in at least one sense: It would diminish the competition in the market for genuine Tiffany merchandise. See id. at 510 n. 36 (noting that "there is at least some basis in the record for eBay's assertion that one of Tiffany's goals in pursuing this litigation is to shut down the legitimate secondary market in authentic Tiffany goods"). The immediate effect would be loss of revenue to eBay, even though there might be a countervailing gain by eBay resulting from increased consumer confidence about the bona fides of other goods sold through its website.

Anti-Counterfeiting Measures

Because eBay facilitates many sales of Tiffany goods, genuine and otherwise, and obtains revenue on every transaction, it generates substantial revenues from the sale of purported Tiffany goods, some of which are counterfeit. "eBay's Jewelry & Watches category manager estimated that, between April 2000 and June 2004, eBay earned $4.1 million in revenue from completed listings with 'Tiffany' in the listing title in the Jewelry & Watches category." Although eBay was generating revenue from all sales of goods on its site, including counterfeit goods, the district court found eBay to have "an interest in eliminating counterfeit Tiffany merchandise from eBay ... to preserve the reputation of its website as a safe place to do business." The buyer of fake Tiffany goods might, if and when the forgery was detected, fault eBay. Indeed, the district court found that "buyers ... complain[ed] to eBay" about the sale of counterfeit Tiffany goods. "[D]uring the last six weeks of 2004, 125 consumers complained to eBay about purchasing 'Tiffany' items through the eBay website that they believed to be counterfeit."

Because eBay "never saw or inspected the merchandise in the listings," its ability to determine whether a particular listing was for counterfeit goods was limited. Even had it been able to

inspect the goods, moreover, in many instances it likely would not have had the expertise to determine whether they were counterfeit.

Notwithstanding these limitations, eBay spent "as much as $20 million each year on tools to promote trust and safety on its website." For example, eBay and PayPal set up "buyer protection programs," under which, in certain circumstances, the buyer would be reimbursed for the cost of items purchased on eBay that were discovered not to be genuine. eBay also established a "Trust and Safety" department, with some 4,000 employees "devoted to trust and safety" issues, including over 200 who "focus exclusively on combating infringement" and 70 who "work exclusively with law enforcement."

By May 2002, eBay had implemented a "fraud engine," "which is principally dedicated to ferreting out illegal listings, including counterfeit listings." eBay had theretofore employed manual searches for keywords in listings in an effort to "identify blatant instances of potentially infringing ... activity." "The fraud engine uses rules and complex models that automatically search for activity that violates eBay policies." In addition to identifying items actually advertised as counterfeit, the engine also incorporates various filters designed to screen out less-obvious instances of counterfeiting using "data elements designed to evaluate listings based on, for example, the seller's Internet protocol address, any issues associated with the seller's account on eBay, and the feedback the seller has received from other eBay users." In addition to general filters, the fraud engine incorporates "Tiffany-specific filters," including "approximately 90 different keywords" designed to help distinguish between genuine and counterfeit Tiffany goods. During the period in dispute, eBay also "periodically conducted [manual] reviews of listings in an effort to remove those that might be selling counterfeit goods, including Tiffany goods."

For nearly a decade, including the period at issue, eBay has also maintained and administered the "Verified Rights Owner ('VeRO') Program"—a "'notice-and-takedown' system" allowing owners of intellectual property rights, including Tiffany, to "report to eBay any listing offering potentially infringing items, so that eBay could remove such reported listings." Any such rights-holder with a "good-faith belief that [a particular listed] item infringed on a copyright or a trademark" could report the item to eBay, using a "Notice Of Claimed Infringement form or NOCI form." During the period under consideration, eBay's practice was to remove reported listings within twenty-four hours of receiving a NOCI, but eBay in fact deleted seventy to eighty percent of them within twelve hours of notification.

On receipt of a NOCI, if the auction or sale had not ended, eBay would, in addition to removing the listing, cancel the bids and inform the seller of the reason for the cancellation. If bidding had ended, eBay would retroactively cancel the transaction. In the event of a cancelled auction, eBay would refund the fees it had been paid in connection with the auction.

In some circumstances, eBay would reimburse the buyer for the cost of a purchased item, provided the buyer presented evidence that the purchased item was counterfeit. During the relevant time period, the district court found, eBay "never refused to remove a reported Tiffany listing, acted in good faith in responding to Tiffany's NOCIs, and always provided Tiffany with the seller's contact information."

In addition, eBay has allowed rights owners such as Tiffany to create an "About Me" webpage on eBay's website "to inform eBay users about their products, intellectual property rights, and legal positions." eBay does not exercise control over the content of those pages in a manner material to the issues before us.

Tiffany, not eBay, maintains the Tiffany "About Me" page. With the headline "**BUYER BEWARE**," the page begins: "**Most of the purported TIFFANY & CO. silver jewelry and packaging available on eBay is counterfeit.**" It also says, *inter alia*:

> The only way you can be certain that you are purchasing a genuine TIFFANY & CO. product is to purchase it from a Tiffany & Co. retail store, via our website (www.tiffany.com) or through a Tiffany & Co. catalogue. Tiffany & Co. stores do not authenticate merchandise. A good jeweler or appraiser may be able to do this for you.

In 2003 or early 2004, eBay began to use "special warning messages when a seller attempted to list a Tiffany item." These messages "instructed the seller to make sure that the item was authentic Tiffany merchandise and informed the seller that eBay 'does not tolerate the listing of replica, counterfeit, or otherwise unauthorized items' and that violation of this policy 'could result in suspension of [the seller's] account.'" The messages also provided a link to Tiffany's "About Me" page with its "buyer beware" disclaimer. If the seller "continued to list an item despite the warning, the listing was flagged for review."

In addition to cancelling particular suspicious transactions, eBay has also suspended from its website "'hundreds of thousands of sellers every year,' tens of thousands of whom were suspected [of] having engaged in infringing conduct." eBay primarily employed a "'three strikes rule'" for suspensions, but would suspend sellers after the first violation if it was clear that "the seller 'listed a number of infringing items,' and '[selling counterfeit merchandise] appears to be the only thing they've come to eBay to do.'" But if "a seller listed a potentially infringing item but appeared overall to be a legitimate seller, the 'infringing items [were] taken down, and the seller [would] be sent a warning on the first offense and given the educational information, [and] told that ... if they do this again, they will be suspended from eBay.'"[5]

By late 2006, eBay had implemented additional anti-fraud measures: delaying the ability of buyers to view listings of certain brand names, including Tiffany's, for 6 to 12 hours so as to give rights-holders such as Tiffany more time to review those listings; developing the ability to assess the number of items listed in a given listing; and restricting one-day and three-day auctions and cross-border trading for some brand-name items.

[5] According to the district court, "eBay took appropriate steps to warn and then to suspend sellers when eBay learned of potential trademark infringement under that seller's account." The district court concluded that it was understandable that eBay did not have a "hard-and-fast, one-strike rule" of suspending sellers because a NOCI "did not constitute a definitive finding that the listed item was counterfeit" and because "suspension was a very serious matter, particularly to those sellers who relied on eBay for their livelihoods." The district court ultimately found eBay's policy to be "appropriate and effective in preventing sellers from returning to eBay and re-listing potentially counterfeit merchandise."

The district court concluded that "eBay consistently took steps to improve its technology and develop anti-fraud measures as such measures became technologically feasible and reasonably available."

eBay's Advertising
At the same time that eBay was attempting to reduce the sale of counterfeit items on its website, it actively sought to promote sales of premium and branded jewelry, including Tiffany merchandise, on its site. Among other things,

> eBay "advised its sellers to take advantage of the demand for Tiffany merchandise as part of a broader effort to grow the Jewelry & Watches category." And prior to 2003, eBay advertised the availability of Tiffany merchandise on its site. eBay's advertisements trumpeted "Mother's Day Gifts!," a "Fall FASHION BRAND BLOWOUT," "Jewelry Best Sellers," "GREAT BRANDS, GREAT PRICES," or "Top Valentine's Deals," among other promotions. It encouraged the viewer to "GET THE FINER THINGS." These advertisements provided the reader with hyperlinks, at least one of each of which was related to Tiffany merchandise—"Tiffany," "Tiffany & Co. under $150," "Tiffany & Co," "Tiffany Rings," or "Tiffany & Co. under $50."

eBay also purchased sponsored-link advertisements on various search engines to promote the availability of Tiffany items on its website. In one such case, in the form of a printout of the results list from a search on Yahoo! for "tiffany," the second sponsored link read "**Tiffany** on eBay. Find **tiffany** items at low prices. With over 5 million items for sale every day, you'll find all kinds of unique [unreadable] Marketplace. www.ebay.com." Tiffany complained to eBay of the practice in 2003, and eBay told Tiffany that it had ceased buying sponsored links. The district court found, however, that eBay continued to do so indirectly through a third party….

DISCUSSION…

I. Direct Trademark Infringement

Tiffany alleges that eBay infringed its trademark in violation of section 32 of the Lanham Act. The district court described this as a claim of "direct trademark infringement," and we adopt that terminology. Under section 32, "the owner of a mark registered with the Patent and Trademark Office can bring a civil action against a person alleged to have used the mark without the owner's consent." We analyze such a claim "under a familiar two-prong test. The test looks first to whether the plaintiff's mark is entitled to protection, and second to whether the defendant's use of the mark is likely to cause consumers confusion as to the origin or sponsorship of the defendant's goods."

In the district court, Tiffany argued that eBay had directly infringed its mark by using it on eBay's website and by purchasing sponsored links containing the mark on Google and Yahoo! Tiffany also argued that eBay and the sellers of the counterfeit goods using its site were jointly and severally liable. The district court rejected these arguments on the ground that eBay's use of Tiffany's mark was protected by the doctrine of nominative fair use.

The doctrine of nominative fair use allows "[a] defendant [to] use a plaintiff's trademark to identify the plaintiff's goods so long as there is no likelihood of confusion about the source of [the] defendant's product or the mark-holder's sponsorship or affiliation." The doctrine apparently originated in the Court of Appeals for the Ninth Circuit. To fall within the protection, according to that court: "First, the product or service in question must be one not readily identifiable without use of the trademark; second, only so much of the mark or marks may be used as is reasonably necessary to identify the product or service; and third, the user must do nothing that would, in conjunction with the mark, suggest sponsorship or endorsement by the trademark holder."

The Court of Appeals for the Third Circuit has endorsed these principles. We have referred to the doctrine, albeit without adopting or rejecting it. Other circuits have done similarly.

We need not address the viability of the doctrine to resolve Tiffany's claim, however. We have recognized that a defendant may lawfully use a plaintiff's trademark where doing so is necessary to describe the plaintiff's product and does not imply a false affiliation or endorsement by the plaintiff of the defendant. "While a trademark conveys an exclusive right to the use of a mark in commerce in the area reserved, that right generally does not prevent one who trades a branded product from accurately describing it by its brand name, so long as the trader does not create confusion by implying an affiliation with the owner of the product."

We agree with the district court that eBay's use of Tiffany's mark on its website and in sponsored links was lawful. eBay used the mark to describe accurately the genuine Tiffany goods offered for sale on its website. And none of eBay's uses of the mark suggested that Tiffany affiliated itself with eBay or endorsed the sale of its products through eBay's website.

In addition, the "About Me" page that Tiffany has maintained on eBay's website since 2004 states that "[m]ost of the purported 'TIFFANY & CO.' silver jewelry and packaging available on eBay is counterfeit." The page further explained that Tiffany itself sells its products only through its own stores, catalogues, and website.

Tiffany argues, however, that even if eBay had the right to use its mark with respect to the resale of genuine Tiffany merchandise, eBay infringed the mark because it knew or had reason to know that there was "a substantial problem with the sale of counterfeit [Tiffany] silver jewelry" on the eBay website. As we discuss below, eBay's knowledge *vel non* that counterfeit Tiffany wares were offered through its website is relevant to the issue of whether eBay contributed to the direct infringement of Tiffany's mark by the counterfeiting vendors themselves, or whether eBay bears liability for false advertising. But it is not a basis for a claim of direct trademark infringement against eBay, especially inasmuch as it is undisputed that eBay promptly removed all listings that Tiffany challenged as counterfeit and took affirmative steps to identify and remove illegitimate Tiffany goods. To impose liability because eBay cannot guarantee the genuineness of all of the purported Tiffany products offered on its website would unduly inhibit the lawful resale of genuine Tiffany goods.

We conclude that eBay's use of Tiffany's mark in the described manner did not constitute direct trademark infringement.

II. Contributory Trademark Infringement

The more difficult issue, and the one that the parties have properly focused our attention on, is whether eBay is liable for contributory trademark infringement—i.e., for culpably facilitating the infringing conduct of the counterfeiting vendors. Acknowledging the paucity of case law to guide us, we conclude that the district court correctly granted judgment on this issue in favor of eBay.

A. Principles

Contributory trademark infringement is a judicially created doctrine that derives from the common law of torts. The Supreme Court most recently dealt with the subject in Inwood Laboratories, Inc. v. Ives Laboratories, Inc., 456 U.S. 844 (1982). There, the plaintiff, Ives, asserted that several drug manufacturers had induced pharmacists to mislabel a drug the defendants produced to pass it off as Ives'. According to the Court, "if a manufacturer or distributor intentionally induces another to infringe a trademark, or if it continues to supply its product to one whom it knows or has reason to know is engaging in trademark infringement, the manufacturer or distributor is contributorially responsible for any harm done as a result of the deceit." The Court ultimately decided to remand the case to the Court of Appeals after concluding it had improperly rejected factual findings of the district court favoring the defendant manufacturers.

Inwood's test for contributory trademark infringement applies on its face to manufacturers and distributors of goods. Courts have, however, extended the test to providers of services.

The Seventh Circuit applied *Inwood* to a lawsuit against the owner of a swap meet, or "flea market," whose vendors were alleged to have sold infringing Hard Rock Café T-shirts. The court "treated trademark infringement as a species of tort," and analogized the swap meet owner to a landlord or licensor, on whom the common law "imposes the same duty ... [as *Inwood*] impose[s] on manufacturers and distributors."

Speaking more generally, the Ninth Circuit concluded that *Inwood's* test for contributory trademark infringement applies to a service provider if he or she exercises sufficient control over the infringing conduct. Lockheed Martin Corp. v. Network Solutions, Inc., 194 F.3d 980, 984 (9th Cir. 1999); see also id. ("Direct control and monitoring of the instrumentality used by a third party to infringe the plaintiff's mark permits the expansion of *Inwood Lab.*'s 'supplies a product' requirement for contributory infringement.").

We have apparently addressed contributory trademark infringement in only two related decisions, and even then in little detail. Citing *Inwood*, we said that "[a] distributor who intentionally induces another to infringe a trademark, or continues to supply its product to one whom it knows or has reason to know is engaging in trademark infringement, is contributorially liable for any injury."

The limited case law leaves the law of contributory trademark infringement ill-defined. Although we are not the first court to consider the application of *Inwood* to the Internet, we are apparently the first to consider its application to an online marketplace.[9]

B. Discussion

1. Does Inwood Apply?

In the district court, the parties disputed whether eBay was subject to the *Inwood* test. eBay argued that it was not because it supplies a service while Inwood governs only manufacturers and distributors of products. The district court rejected that distinction. It adopted instead the reasoning of the Ninth Circuit in *Lockheed* to conclude that Inwood applies to a service provider who exercises sufficient control over the means of the infringing conduct. Looking "to the extent of the control exercised by eBay over its sellers' means of infringement," the district court concluded that *Inwood* applied in light of the "significant control" eBay retained over the transactions and listings facilitated by and conducted through its website.

On appeal, eBay no longer maintains that it is not subject to Inwood. We therefore assume without deciding that *Inwood's* test for contributory trademark infringement governs.

2. Is eBay Liable Under Inwood?

The question that remains, then, is whether eBay is liable under the *Inwood* test on the basis of the services it provided to those who used its website to sell counterfeit Tiffany products. As noted, when applying *Inwood* to service providers, there are two ways in which a defendant may become contributorially liable for the infringing conduct of another: first, if the service provider "intentionally induces another to infringe a trademark," and second, if the service provider "continues to supply its [service] to one whom it knows or has reason to know is engaging in trademark infringement." Inwood, 456 U.S. at 854. Tiffany does not argue that eBay induced the sale of counterfeit Tiffany goods on its website-the circumstances addressed by the first part of the *Inwood* test. It argues instead, under the second part of the *Inwood* test, that eBay continued to supply its services to the sellers of counterfeit Tiffany goods while knowing or having reason to know that such sellers were infringing Tiffany's mark.

The district court rejected this argument. First, it concluded that to the extent the NOCIs that Tiffany submitted gave eBay reason to know that particular listings were for counterfeit goods, eBay did not continue to carry those listings once it learned that they were specious. The court found that eBay's practice was promptly to remove the challenged listing from its website, warn sellers and buyers, cancel fees it earned from that listing, and direct buyers not to consummate the sale of the disputed item. The court therefore declined to hold eBay contributorially liable for the infringing conduct of those sellers. On appeal, Tiffany does not appear to challenge this conclusion. In any event, we agree with the district court that no liability arises with respect to those terminated listings.

[9] European courts have done so. A Belgian court declined to hold eBay liable for counterfeit cosmetic products sold through its website. French courts, by contrast, have concluded that eBay violated applicable trademark laws.

Tiffany disagrees vigorously, however, with the district court's further determination that eBay lacked sufficient knowledge of trademark infringement by sellers behind other, non-terminated listings to provide a basis for Inwood liability. Tiffany argued in the district court that eBay knew, or at least had reason to know, that counterfeit Tiffany goods were being sold ubiquitously on its website. As evidence, it pointed to, *inter alia*, the demand letters it sent to eBay in 2003 and 2004, the results of its Buying Programs that it shared with eBay, the thousands of NOCIs it filed with eBay alleging its good faith belief that certain listings were counterfeit, and the various complaints eBay received from buyers claiming that they had purchased one or more counterfeit Tiffany items through eBay's website. Tiffany argued that taken together, this evidence established eBay's knowledge of the widespread sale of counterfeit Tiffany products on its website. Tiffany urged that eBay be held contributorially liable on the basis that despite that knowledge, it continued to make its services available to infringing sellers.

The district court rejected this argument. It acknowledged that "[t]he evidence produced at trial demonstrated that eBay had *generalized* notice that some portion of the Tiffany goods sold on its website might be counterfeit." The court characterized the issue before it as "whether eBay's *generalized* knowledge of trademark infringement on its website was sufficient to meet the 'knowledge or reason to know' prong of the *Inwood* test." eBay had argued that "such generalized knowledge is insufficient, and that the law demands more specific knowledge of individual instances of infringement and infringing sellers before imposing a burden upon eBay to remedy the problem."

The district court concluded that "while eBay clearly possessed general knowledge as to counterfeiting on its website, such generalized knowledge is insufficient under the Inwood test to impose upon eBay an affirmative duty to remedy the problem." The court reasoned that Inwood's language explicitly imposes contributory liability on a defendant who "continues to supply its product [—in eBay's case, its service—] to *one* whom it knows or has reason to know is engaging in trademark infringement." The court also noted that plaintiffs "bear a high burden in establishing 'knowledge' of contributory infringement," and that courts have

> been reluctant to extend contributory trademark liability to defendants where there is some uncertainty as to the extent or the nature of the infringement. In *Inwood*, Justice White emphasized in his concurring opinion that a defendant is not "require[d] ... to refuse to sell to dealers who merely *might* pass off its goods."

Accordingly, the district court concluded that for Tiffany to establish eBay's contributory liability, Tiffany would have to show that eBay "knew or had reason to know of specific instances of actual infringement" beyond those that it addressed upon learning of them. Tiffany failed to make such a showing.

On appeal, Tiffany argues that the distinction drawn by the district court between eBay's general knowledge of the sale of counterfeit Tiffany goods through its website, and its specific knowledge as to which particular sellers were making such sales, is a "false" one not required by the law. Tiffany posits that the only relevant question is "whether all of the knowledge, when taken together, puts [eBay] on notice that there is a substantial problem of trademark infringement. If so and if it fails to act, [eBay] is liable for contributory trademark infringement."

We agree with the district court. For contributory trademark infringement liability to lie, a service provider must have more than a general knowledge or reason to know that its service is being used to sell counterfeit goods. Some contemporary knowledge of which particular listings are infringing or will infringe in the future is necessary.

We are not persuaded by Tiffany's proposed interpretation of *Inwood*. Tiffany understands the "lesson of *Inwood*" to be that an action for contributory trademark infringement lies where "the evidence [of infringing activity]—direct or circumstantial, taken as a whole—... provide[s] a basis for finding that the defendant knew or should have known that its product or service was being used to further illegal counterfeiting activity." We think that Tiffany reads *Inwood* too broadly. Although the *Inwood* Court articulated a "knows or has reason to know" prong in setting out its contributory liability test, the Court explicitly declined to apply that prong to the facts then before it. The Court applied only the inducement prong of the test.

We therefore do not think that *Inwood* establishes the contours of the "knows or has reason to know" prong. Insofar as it speaks to the issue, though, the particular phrasing that the Court used—that a defendant will be liable if it "continues to supply its product to *one* whom it knows or has reason to know is engaging in trademark infringement" (emphasis added)—supports the district court's interpretation of *Inwood*, not Tiffany's.

We find helpful the Supreme Court's discussion of *Inwood* in a subsequent *copyright* case, Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984). There, defendant Sony manufactured and sold home video tape recorders. Plaintiffs Universal Studios and Walt Disney Productions held copyrights on various television programs that individual television-viewers had taped using the defendant's recorders. The plaintiffs contended that this use of the recorders constituted copyright infringement for which the defendants should be held contributorily liable. In ruling for the defendants, the Court discussed *Inwood* and the differences between contributory liability in trademark versus copyright law.

> If *Inwood's narrow standard* for contributory trademark infringement governed here, [the plaintiffs'] claim of contributory infringement would merit little discussion. Sony certainly does not 'intentionally induce[ ]' its customers to make infringing uses of [the plaintiffs'] copyrights, nor does it supply its products to *identified individuals known by it* to be engaging in continuing infringement of [the plaintiffs'] copyrights.

(emphases added).

Thus, the Court suggested, had the *Inwood* standard applied in *Sony*, the fact that Sony might have known that some portion of the purchasers of its product used it to violate the copyrights of others would not have provided a sufficient basis for contributory liability. *Inwood's* "narrow standard" would have required knowledge by Sony of "identified individuals" engaging in infringing conduct. Tiffany's reading of *Inwood* is therefore contrary to the interpretation of that case set forth in *Sony*.

Although the Supreme Court's observations in *Sony*, a copyright case, about the "knows or has reason to know" prong of the contributory trademark infringement test set forth in *Inwood* were dicta, they constitute the only discussion of that prong by the Supreme Court of which we are aware. We think them to be persuasive authority here.

Applying *Sony's* interpretation of *Inwood*, we agree with the district court that "Tiffany's general allegations of counterfeiting failed to provide eBay with the knowledge required under *Inwood*." Tiffany's demand letters and Buying Programs did not identify particular sellers who Tiffany thought were then offering or would offer counterfeit goods.[13] And although the NOCIs and buyer complaints gave eBay reason to know that certain sellers had been selling counterfeits, those sellers' listings were removed and repeat offenders were suspended from the eBay site. Thus Tiffany failed to demonstrate that eBay was supplying its service to individuals who it knew or had reason to know were selling counterfeit Tiffany goods.

Accordingly, we affirm the judgment of the district court insofar as it holds that eBay is not contributorially liable for trademark infringement.

3. Willful Blindness.

Tiffany and its amici express their concern that if eBay is not held liable except when specific counterfeit listings are brought to its attention, eBay will have no incentive to root out such listings from its website. They argue that this will effectively require Tiffany and similarly situated retailers to police eBay's website—and many others like it—"24 hours a day, and 365 days a year." They urge that this is a burden that most mark holders cannot afford to bear.

First, and most obviously, we are interpreting the law and applying it to the facts of this case. We could not, even if we thought it wise, revise the existing law in order to better serve one party's interests at the expense of the other's.

But we are also disposed to think, and the record suggests, that private market forces give eBay and those operating similar businesses a strong incentive to minimize the counterfeit goods sold on their websites. eBay received many complaints from users claiming to have been duped into buying counterfeit Tiffany products sold on eBay. The risk of alienating these users gives eBay a reason to identify and remove counterfeit listings.[14] Indeed, it has spent millions of dollars in that effort.

Moreover, we agree with the district court that if eBay had reason to suspect that counterfeit Tiffany goods were being sold through its website, and intentionally shielded itself from discovering the offending listings or the identity of the sellers behind them, eBay might very well have been charged with knowledge of those sales sufficient to satisfy *Inwood's* "knows or has reason to know" prong. A service provider is not, we think, permitted willful blindness. When it has reason to suspect that users of its service are infringing a protected mark, it may not shield

[13] The demand letters did say that eBay should presume that sellers offering five or more Tiffany goods were selling counterfeits, but we agree with the district court that this presumption was factually unfounded.

[14] At the same time, we appreciate the argument that insofar as eBay receives revenue from undetected counterfeit listings and sales through the fees it charges, it has an incentive to permit such listings and sales to continue.

itself from learning of the particular infringing transactions by looking the other way.[15] In the words of the Seventh Circuit, "willful blindness is equivalent to actual knowledge for purposes of the Lanham Act."

eBay appears to concede that it knew as a general matter that counterfeit Tiffany products were listed and sold through its website. Without more, however, this knowledge is insufficient to trigger liability under *Inwood*. The district court found, after careful consideration, that eBay was not willfully blind to the counterfeit sales. That finding is not clearly erroneous.[17] eBay did not ignore the information it was given about counterfeit sales on its website.

III. Trademark Dilution…

The district court rejected Tiffany's dilution by blurring claim on the ground that "eBay never used the TIFFANY Marks in an effort to create an association with its own product, but instead, used the marks directly to advertise and identify the availability of authentic Tiffany merchandise on the eBay website." The court concluded that "just as the dilution by blurring claim fails because eBay has never used the [Tiffany] Marks to refer to eBay's own product, the dilution by tarnishment claim also fails."

We agree. There is no second mark or product at issue here to blur with or to tarnish "Tiffany."

Tiffany argues that counterfeiting dilutes the value of its product. Perhaps. But insofar as eBay did not itself sell the goods at issue, it did not itself engage in dilution….

IV. False Advertising

Finally, Tiffany claims that eBay engaged in false advertising in violation of federal law.

A. Principles

Section 43(a) of the Lanham Act prohibits any person from, "in commercial advertising or promotion, misrepresent[ing] the nature, characteristics, qualities, or geographic origin of his or her or another person's goods, services, or commercial activities." A claim of false advertising may be based on at least one of two theories: "that the challenged advertisement is literally false, i.e., false on its face," or "that the advertisement, while not literally false, is nevertheless likely to mislead or confuse consumers."

---

[15] To be clear, a service provider is not contributorially liable under *Inwood* merely for failing to anticipate that others would use its service to infringe a protected mark. But contributory liability may arise where a defendant is (as was eBay here) made aware that there was infringement on its site but (unlike eBay here) ignored that fact.

[17] Tiffany's reliance on the "flea market" cases, *Hard Rock Café* and *Fonovisa*, is unavailing. eBay's efforts to combat counterfeiting far exceeded the efforts made by the defendants in those cases. See Hard Rock Café, 955 F.2d at 1146 (defendant did not investigate any of the seizures of counterfeit products at its swap meet, even though it knew they had occurred); Fonovisa, 76 F.3d at 265 (concluding that plaintiff stated a claim for contributory trademark infringement based on allegation that swap meet "disregard[ed] its vendors' blatant trademark infringements with impunity"). Moreover, neither case concluded that the defendant was willfully blind. The court in *Hard Rock Café* remanded so that the district court could apply the correct definition of "willful blindness," and the court in *Fonovisa* merely sustained the plaintiff's complaint against a motion to dismiss.

In either case, the "injuries redressed in false advertising cases are the result of public deception." And "[u]nder either theory, the plaintiff must also demonstrate that the false or misleading representation involved an inherent or material quality of the product."

Where an advertising claim is literally false, "the court may enjoin the use of the claim without reference to the advertisement's impact on the buying public." To succeed in a likelihood-of-confusion case where the statement at issue is not literally false, however, a plaintiff "must demonstrate, by extrinsic evidence, that the challenged commercials tend to mislead or confuse consumers," and must "demonstrate that a statistically significant part of the commercial audience holds the false belief allegedly communicated by the challenged advertisement."

B. Discussion

eBay advertised the sale of Tiffany goods on its website in various ways. Among other things, eBay provided hyperlinks to "Tiffany," "Tiffany & Co. under $150," "Tiffany & Co.," "Tiffany Rings," and "Tiffany & Co. under $50." eBay also purchased advertising space on search engines, in some instances providing a link to eBay's site and exhorting the reader to "Find **tiffany** items at low prices." Yet the district court found, and eBay does not deny, that "eBay certainly had generalized knowledge that Tiffany products sold on eBay were often counterfeit." Tiffany argues that because eBay advertised the sale of Tiffany goods on its website, and because many of those goods were in fact counterfeit, eBay should be liable for false advertising.

The district court rejected this argument. The court first concluded that the advertisements at issue were not literally false "[b]ecause authentic Tiffany merchandise is sold on eBay's website," even if counterfeit Tiffany products are sold there, too.

The court then considered whether the advertisements, though not literally false, were nonetheless misleading. It concluded they were not for three reasons. First, the court found that eBay's use of Tiffany's mark in its advertising was "protected, nominative fair use." Second, the court found that "Tiffany has not proven that eBay had specific knowledge as to the illicit nature of individual listings," implying that such knowledge would be necessary to sustain a false advertising claim. Finally, the court reasoned that "to the extent that the advertising was false, the falsity was the responsibility of third party sellers, not eBay."

We agree with the district court that eBay's advertisements were not literally false inasmuch as genuine Tiffany merchandise was offered for sale through eBay's website. But we are unable to affirm on the record before us the district court's further conclusion that eBay's advertisements were not "likely to mislead or confuse consumers."

As noted, to evaluate Tiffany's claim that eBay's advertisements misled consumers, a court must determine whether extrinsic evidence indicates that the challenged advertisements were misleading or confusing. The reasons the district court gave for rejecting Tiffany's claim do not seem to reflect this determination, though. The court's first rationale was that eBay's advertisements were nominative fair use of Tiffany's mark.

But, even if that is so, it does not follow that eBay did not use the mark in a misleading advertisement. It may, after all, constitute fair use for Brand X Coffee to use the trademark of its competitor, Brand Y Coffee, in an advertisement stating that "In a blind taste test, 9 out of 10 New Yorkers said they preferred Brand X Coffee to Brand Y Coffee." But if 9 out of 10 New Yorkers in a statistically significant sample did not say they preferred X to Y, or if they were paid to say that they did, then the advertisement would nonetheless be literally false in the first example, or misleading in the second.

There is a similar difficulty with the district court's reliance on the fact that eBay did not know which particular listings on its website offered counterfeit Tiffany goods. That is relevant, as we have said, to whether eBay committed contributory trademark infringement. But it sheds little light on whether the advertisements were misleading insofar as they implied the genuineness of Tiffany goods on eBay's site.

Finally, the district court reasoned that if eBay's advertisements were misleading, that was only because the sellers of counterfeits made them so by offering inauthentic Tiffany goods. Again, this consideration is relevant to Tiffany's direct infringement claim, but less relevant, if relevant at all, here. It is true that eBay did not itself sell counterfeit Tiffany goods; only the fraudulent vendors did, and that is in part why we conclude that eBay did not infringe Tiffany's mark. But eBay did affirmatively advertise the goods sold through its site as Tiffany merchandise. The law requires us to hold eBay accountable for the words that it chose insofar as they misled or confused consumers.

eBay and its amici warn of the deterrent effect that will grip online advertisers who are unable to confirm the authenticity of all of the goods they advertise for sale. We rather doubt that the consequences will be so dire. An online advertiser such as eBay need not cease its advertisements for a kind of goods only because it knows that not all of those goods are authentic. A disclaimer might suffice. But the law prohibits an advertisement that implies that all of the goods offered on a defendant's website are genuine when in fact, as here, a sizeable proportion of them are not.

Rather than vacate the judgment of the district court as to Tiffany's false advertising claim, we think it prudent to remand the cause so that the district court, with its greater familiarity with the evidence, can reconsider the claim in light of what we have said. The case is therefore remanded…for further proceedings for the limited purpose of the district court's re-examination of the false advertising claim in accordance with this opinion….

Pornography Glossary

Obscenity is: "(a) whether the average person, applying contemporary community standards, would find that the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political or scientific value." [Miller]

Indecency is: "language that describes, in terms patently offensive as measured by contemporary community standards for the broadcast medium, sexual or excretory activities and organs, at times of the day when there is a reasonable risk that children may be in the audience." [FCC definition, quoted in Pacifica]

> Compare the CDA: "any comment, request, suggestion, proposal, image or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs."

Harmful to minor is: "(a) patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors; (b) appeals to the prurient interests of minors; and (c) is utterly without redeeming social importance for minors." [Ginsberg]

> Compare COPA: "any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that is obscene or that (A) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest; (B) depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and (C) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors."

Child pornography is: "works that visually depict sexual conduct by children below a specified age, where the category of "sexual conduct" proscribed is suitably limited and described." [Ferber] In the New York statute's case, "sexual conduct" was defined as "actual or simulated sexual intercourse, deviate sexual intercourse, sexual bestiality, masturbation, sado-masochistic abuse, or lewd exhibition of the genitals."

Pornography is: ?????

Reno v. American Civil Liberties Union, 521 U.S. 844 (1997).
Stevens, Justice.

At issue is the constitutionality of two statutory provisions enacted to protect minors from "indecent" and "patently offensive" communications on the Internet. Notwithstanding the legitimacy and importance of the congressional goal of protecting children from harmful materials, we agree with the three-judge District Court that the statute abridges "the freedom of speech" protected by the First Amendment.

I

The District Court made extensive findings of fact, most of which were based on a detailed stipulation prepared by the parties. The findings describe the character and the dimensions of the Internet, the availability of sexually explicit material in that medium, and the problems confronting age verification for recipients of Internet communications. Because those findings provide the underpinnings for the legal issues, we begin with a summary of the undisputed facts.

The Internet
The Internet is an international network of interconnected computers. It is the outgrowth of what began in 1969 as a military program called "ARPANET," which was designed to enable computers operated by the military, defense contractors, and universities conducting defense-related research to communicate with one another by redundant channels even if some portions of the network were damaged in a war. While the ARPANET no longer exists, it provided an example for the development of a number of civilian networks that, eventually linking with each other, now enable tens of millions of people to communicate with one another and to access vast amounts of information from around the world. The Internet is "a unique and wholly new medium of worldwide human communication."

The Internet has experienced "extraordinary growth." The number of "host" computers—those that store information and relay communications—increased from about 300 in 1981 to approximately 9,400,000 by the time of the trial in 1996. Roughly 60% of these hosts are located in the United States. About 40 million people used the Internet at the time of trial, a number that is expected to mushroom to 200 million by 1999.

Individuals can obtain access to the Internet from many different sources, generally hosts themselves or entities with a host affiliation. Most colleges and universities provide access for their students and faculty; many corporations provide their employees with access through an office network; many communities and local libraries provide free access; and an increasing number of storefront "computer coffee shops" provide access for a small hourly fee. Several major national "online services" such as America Online, CompuServe, the Microsoft Network, and Prodigy offer access to their own extensive proprietary networks as well as a link to the much larger resources of the Internet. These commercial online services had almost 12 million individual subscribers at the time of trial.

Anyone with access to the Internet may take advantage of a wide variety of communication and information retrieval methods. These methods are constantly evolving and difficult to categorize

precisely. But, as presently constituted, those most relevant to this case are electronic mail (e-mail), automatic mailing list services ("mail exploders," sometimes referred to as "listservs"), "newsgroups," "chat rooms," and the "World Wide Web." All of these methods can be used to transmit text; most can transmit sound, pictures, and moving video images. Taken together, these tools constitute a unique medium—known to its users as "cyberspace"—located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet.

E-mail enables an individual to send an electronic message—generally akin to a note or letter—to another individual or to a group of addressees. The message is generally stored electronically, sometimes waiting for the recipient to check her "mailbox" and sometimes making its receipt known through some type of prompt. A mail exploder is a sort of e-mail group. Subscribers can send messages to a common e-mail address, which then forwards the message to the group's other subscribers. Newsgroups also serve groups of regular participants, but these postings may be read by others as well. There are thousands of such groups, each serving to foster an exchange of information or opinion on a particular topic running the gamut from, say, the music of Wagner to Balkan politics to AIDS prevention to the Chicago Bulls. About 100,000 new messages are posted every day. In most newsgroups, postings are automatically purged at regular intervals. In addition to posting a message that can be read later, two or more individuals wishing to communicate more immediately can enter a chat room to engage in real-time dialogue—in other words, by typing messages to one another that appear almost immediately on the others' computer screens. The District Court found that at any given time "tens of thousands of users are engaging in conversations on a huge range of subjects." It is "no exaggeration to conclude that the content on the Internet is as diverse as human thought."

The best known category of communication over the Internet is the World Wide Web, which allows users to search for and retrieve information stored in remote computers, as well as, in some cases, to communicate back to designated sites. In concrete terms, the Web consists of a vast number of documents stored in different computers all over the world. Some of these documents are simply files containing information. However, more elaborate documents, commonly known as Web "pages," are also prevalent. Each has its own address—"rather like a telephone number." Web pages frequently contain information and sometimes allow the viewer to communicate with the page's (or "site's") author. They generally also contain "links" to other documents created by that site's author or to other (generally) related sites. Typically, the links are either blue or underlined text—sometimes images.

Navigating the Web is relatively straightforward. A user may either type the address of a known page or enter one or more keywords into a commercial "search engine" in an effort to locate sites on a subject of interest. A particular Web page may contain the information sought by the "surfer," or, through its links, it may be an avenue to other documents located anywhere on the Internet. Users generally explore a given Web page, or move to another, by clicking a computer "mouse" on one of the page's icons or links. Access to most Web pages is freely available, but some allow access only to those who have purchased the right from a commercial provider. The Web is thus comparable, from the readers' viewpoint, to both a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and services.

From the publishers' point of view, it constitutes a vast platform from which to address and hear from a worldwide audience of millions of readers, viewers, researchers, and buyers. Any person or organization with a computer connected to the Internet can "publish" information. Publishers include government agencies, educational institutions, commercial entities, advocacy groups, and individuals. Publishers may either make their material available to the entire pool of Internet users, or confine access to a selected group, such as those willing to pay for the privilege. "No single organization controls any membership in the Web, nor is there any single centralized point from which individual Web sites or services can be blocked from the Web."

Sexually Explicit Material

Sexually explicit material on the Internet includes text, pictures, and chat and "extends from the modestly titillating to the hardest-core." These files are created, named, and posted in the same manner as material that is not sexually explicit, and may be accessed either deliberately or unintentionally during the course of an imprecise search. "Once a provider posts its content on the Internet, it cannot prevent that content from entering any community." Thus, for example,

> "when the UCR/California Museum of Photography posts to its Web site nudes by Edward Weston and Robert Mapplethorpe to announce that its new exhibit will travel to Baltimore and New York City, those images are available not only in Los Angeles, Baltimore, and New York City, but also in Cincinnati, Mobile, or Beijing—wherever Internet users live. Similarly, the safer sex instructions that Critical Path posts to its Web site, written in street language so that the teenage receiver can understand them, are available not just in Philadelphia, but also in Provo and Prague."

Some of the communications over the Internet that originate in foreign countries are also sexually explicit.

Though such material is widely available, users seldom encounter such content accidentally. "A document's title or a description of the document will usually appear before the document itself ... and in many cases the user will receive detailed information about a site's content before he or she need take the step to access the document. Almost all sexually explicit images are preceded by warnings as to the content." For that reason, the "odds are slim" that a user would enter a sexually explicit site by accident. Unlike communications received by radio or television, "the receipt of information on the Internet requires a series of affirmative steps more deliberate and directed than merely turning a dial. A child requires some sophistication and some ability to read to retrieve material and thereby to use the Internet unattended."

Systems have been developed to help parents control the material that may be available on a home computer with Internet access. A system may either limit a computer's access to an approved list of sources that have been identified as containing no adult material, it may block designated inappropriate sites, or it may attempt to block messages containing identifiable objectionable features. "Although parental control software currently can screen for certain suggestive words or for known sexually explicit sites, it cannot now screen for sexually explicit images." Nevertheless, the evidence indicates that "a reasonably effective method by which

parents can prevent their children from accessing sexually explicit and other material which parents may believe is inappropriate for their children will soon be widely available."

Age Verification

The problem of age verification differs for different uses of the Internet. The District Court categorically determined that there "is no effective way to determine the identity or the age of a user who is accessing material through e-mail, mail exploders, newsgroups or chat rooms." The Government offered no evidence that there was a reliable way to screen recipients and participants in such forums for age. Moreover, even if it were technologically feasible to block minors' access to newsgroups and chat rooms containing discussions of art, politics, or other subjects that potentially elicit "indecent" or "patently offensive" contributions, it would not be possible to block their access to that material and "still allow them access to the remaining content, even if the overwhelming majority of that content was not indecent."

Technology exists by which an operator of a Web site may condition access on the verification of requested information such as a credit card number or an adult password. Credit card verification is only feasible, however, either in connection with a commercial transaction in which the card is used, or by payment to a verification agency. Using credit card possession as a surrogate for proof of age would impose costs on non-commercial Web sites that would require many of them to shut down. For that reason, at the time of the trial, credit card verification was "effectively unavailable to a substantial number of Internet content providers." Moreover, the imposition of such a requirement "would completely bar adults who do not have a credit card and lack the resources to obtain one from accessing any blocked material."

Commercial pornographic sites that charge their users for access have assigned them passwords as a method of age verification. The record does not contain any evidence concerning the reliability of these technologies. Even if passwords are effective for commercial purveyors of indecent material, the District Court found that an adult password requirement would impose significant burdens on noncommercial sites, both because they would discourage users from accessing their sites and because the cost of creating and maintaining such screening systems would be "beyond their reach."

In sum, the District Court found:

> "Even if credit card verification or adult password verification were implemented, the Government presented no testimony as to how such systems could ensure that the user of the password or credit card is in fact over 18. The burdens imposed by credit card verification and adult password verification systems make them effectively unavailable to a substantial number of Internet content providers."

II

The Telecommunications Act of 1996 was an unusually important legislative enactment. As stated on the first of its 103 pages, its primary purpose was to reduce regulation and encourage "the rapid deployment of new telecommunications technologies." The major components of the statute have nothing to do with the Internet; they were designed to promote competition in the

local telephone service market, the multichannel video market, and the market for over-the-air broadcasting. The Act includes seven Titles, six of which are the product of extensive committee hearings and the subject of discussion in Reports prepared by Committees of the Senate and the House of Representatives. By contrast, Title V—known as the "Communications Decency Act of 1996" (CDA)—contains provisions that were either added in executive committee after the hearings were concluded or as amendments offered during floor debate on the legislation. An amendment offered in the Senate was the source of the two statutory provisions challenged in this case. They are informally described as the "indecent transmission" provision and the "patently offensive display" provision.

The first, 47 U.S.C. § 223(a) (1994 ed., Supp. II), prohibits the knowing transmission of obscene or indecent messages to any recipient under 18 years of age. It provides in pertinent part:

> "(a) Whoever-
> "(1) in interstate or foreign communications-
> . . . . .
> "(B) by means of a telecommunications device knowingly-
> "(i) makes, creates, or solicits, and
> "(ii) initiates the transmission of,
> "any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age, regardless of whether the maker of such communication placed the call or initiated the communication;
> . . . . .
> "(2) knowingly permits any telecommunications facility under his control to be used for any activity prohibited by paragraph (1) with the intent that it be used for such activity,
> "shall be fined under Title 18, or imprisoned not more than two years, or both."

The second provision, § 223(d), prohibits the knowing sending or displaying of patently offensive messages in a manner that is available to a person under 18 years of age. It provides:

> "(d) Whoever-
> "(1) in interstate or foreign communications knowingly-
> "(A) uses an interactive computer service to send to a specific person or persons under 18 years of age, or
> "(B) uses any interactive computer service to display in a manner available to a person under 18 years of age,
> "any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication; or
> "(2) knowingly permits any telecommunications facility under such person's control to be used for an activity prohibited by paragraph (1) with the intent that it be used for such activity,

"shall be fined under Title 18, or imprisoned not more than two years, or both."

The breadth of these prohibitions is qualified by two affirmative defenses. One covers those who take "good faith, reasonable, effective, and appropriate actions" to restrict access by minors to the prohibited communications. § 223(e)(5)(A). The other covers those who restrict access to covered material by requiring certain designated forms of age proof, such as a verified credit card or an adult identification number or code. § 223(e)(5)(B)….

IV

In arguing for reversal, the Government contends that the CDA is plainly constitutional under three of our prior decisions: (1) Ginsberg v. New York, 390 U.S. 629 (1968); (2) FCC v. Pacifica Foundation, 438 U.S. 726, (1978); and (3) Renton v. Playtime Theatres, Inc., 475 U.S. 41 (1986). A close look at these cases, however, raises—rather than relieves—doubts concerning the constitutionality of the CDA.

In *Ginsberg*, we upheld the constitutionality of a New York statute that prohibited selling to minors under 17 years of age material that was considered obscene as to them even if not obscene as to adults. We rejected the defendant's broad submission that "the scope of the constitutional freedom of expression secured to a citizen to read or see material concerned with sex cannot be made to depend on whether the citizen is an adult or a minor." In rejecting that contention, we relied not only on the State's independent interest in the well-being of its youth, but also on our consistent recognition of the principle that "the parents' claim to authority in their own household to direct the rearing of their children is basic in the structure of our society."

In four important respects, the statute upheld in *Ginsberg* was narrower than the CDA. First, we noted in Ginsberg that "the prohibition against sales to minors does not bar parents who so desire from purchasing the magazines for their children." Under the CDA, by contrast, neither the parents' consent—nor even their participation—in the communication would avoid the application of the statute. Second, the New York statute applied only to commercial transactions, whereas the CDA contains no such limitation. Third, the New York statute cabined its definition of material that is harmful to minors with the requirement that it be "utterly without redeeming social importance for minors." The CDA fails to provide us with any definition of the term "indecent" as used in § 223(a)(1) and, importantly, omits any requirement that the "patently offensive" material covered by § 223(d) lack serious literary, artistic, political, or scientific value. Fourth, the New York statute defined a minor as a person under the age of 17, whereas the CDA, in applying to all those under 18 years, includes an additional year of those nearest majority.

In *Pacifica*, we upheld a declaratory order of the Federal Communications Commission, holding that the broadcast of a recording of a 12-minute monologue entitled "Filthy Words" that had previously been delivered to a live audience "could have been the subject of administrative sanctions." The Commission had found that the repetitive use of certain words referring to excretory or sexual activities or organs "in an afternoon broadcast when children are in the audience was patently offensive" and concluded that the monologue was indecent "as broadcast." The respondent did not quarrel with the finding that the afternoon broadcast was

patently offensive, but contended that it was not "indecent" within the meaning of the relevant statutes because it contained no prurient appeal. After rejecting respondent's statutory arguments, we confronted its two constitutional arguments: (1) that the Commission's construction of its authority to ban indecent speech was so broad that its order had to be set aside even if the broadcast at issue was unprotected; and (2) that since the recording was not obscene, the First Amendment forbade any abridgment of the right to broadcast it on the radio.

In the portion of the lead opinion not joined by Justices Powell and Blackmun, the plurality stated that the First Amendment does not prohibit all governmental regulation that depends on the content of speech. Accordingly, the availability of constitutional protection for a vulgar and offensive monologue that was not obscene depended on the context of the broadcast. Relying on the premise that "of all forms of communication" broadcasting had received the most limited First Amendment protection, the Court concluded that the ease with which children may obtain access to broadcasts, "coupled with the concerns recognized in Ginsberg," justified special treatment of indecent broadcasting.

As with the New York statute at issue in *Ginsberg*, there are significant differences between the order upheld in *Pacifica* and the CDA. First, the order in *Pacifica*, issued by an agency that had been regulating radio stations for decades, targeted a specific broadcast that represented a rather dramatic departure from traditional program content in order to designate when—rather than whether—it would be permissible to air such a program in that particular medium. The CDA's broad categorical prohibitions are not limited to particular times and are not dependent on any evaluation by an agency familiar with the unique characteristics of the Internet. Second, unlike the CDA, the Commission's declaratory order was not punitive; we expressly refused to decide whether the indecent broadcast "would justify a criminal prosecution." Finally, the Commission's order applied to a medium which as a matter of history had "received the most limited First Amendment protection," in large part because warnings could not adequately protect the listener from unexpected program content. The Internet, however, has no comparable history. Moreover, the District Court found that the risk of encountering indecent material by accident is remote because a series of affirmative steps is required to access specific material.

In *Renton*, we upheld a zoning ordinance that kept adult movie theaters out of residential neighborhoods. The ordinance was aimed, not at the content of the films shown in the theaters, but rather at the "secondary effects"—such as crime and deteriorating property values—that these theaters fostered: "'It is th[e] secondary effect which these zoning ordinances attempt to avoid, not the dissemination of "offensive" speech.'" According to the Government, the CDA is constitutional because it constitutes a sort of "cyberzoning" on the Internet. But the CDA applies broadly to the entire universe of cyberspace. And the purpose of the CDA is to protect children from the primary effects of "indecent" and "patently offensive" speech, rather than any "secondary" effect of such speech. Thus, the CDA is a content-based blanket restriction on speech, and, as such, cannot be "properly analyzed as a form of time, place, and manner regulation."

These precedents, then, surely do not require us to uphold the CDA and are fully consistent with the application of the most stringent review of its provisions.

V

In Southeastern Promotions, Ltd. v. Conrad, 420 U.S. 546, 557 (1975), we observed that "[e]ach medium of expression ... may present its own problems." Thus, some of our cases have recognized special justifications for regulation of the broadcast media that are not applicable to other speakers. In these cases, the Court relied on the history of extensive Government regulation of the broadcast medium; the scarcity of available frequencies at its inception; and its "invasive" nature.

Those factors are not present in cyberspace. Neither before nor after the enactment of the CDA have the vast democratic forums of the Internet been subject to the type of government supervision and regulation that has attended the broadcast industry. Moreover, the Internet is not as "invasive" as radio or television. The District Court specifically found that "[c]ommunications over the Internet do not 'invade' an individual's home or appear on one's computer screen unbidden. Users seldom encounter content 'by accident.'" It also found that "[a]lmost all sexually explicit images are preceded by warnings as to the content," and cited testimony that "'odds are slim' that a user would come across a sexually explicit sight by accident."

We distinguished *Pacifica* in *Sable*, 492 U.S., at 128, on just this basis. In *Sable*, a company engaged in the business of offering sexually oriented prerecorded telephone messages (popularly known as "dial-a-porn") challenged the constitutionality of an amendment to the Communications Act of 1934 that imposed a blanket prohibition on indecent as well as obscene interstate commercial telephone messages. We held that the statute was constitutional insofar as it applied to obscene messages but invalid as applied to indecent messages. In attempting to justify the complete ban and criminalization of indecent commercial telephone messages, the Government relied on *Pacifica*, arguing that the ban was necessary to prevent children from gaining access to such messages. We agreed that "there is a compelling interest in protecting the physical and psychological well-being of minors" which extended to shielding them from indecent messages that are not obscene by adult standards, but distinguished our "emphatically narrow holding" in *Pacifica* because it did not involve a complete ban and because it involved a different medium of communication. We explained that "the dial-it medium requires the listener to take affirmative steps to receive the communication." "Placing a telephone call," we continued, "is not the same as turning on a radio and being taken by surprise by an indecent message."

Finally, unlike the conditions that prevailed when Congress first authorized regulation of the broadcast spectrum, the Internet can hardly be considered a "scarce" expressive commodity. It provides relatively unlimited, low-cost capacity for communication of all kinds. The Government estimates that "[a]s many as 40 million people use the Internet today, and that figure is expected to grow to 200 million by 1999." This dynamic, multifaceted category of communication includes not only traditional print and news services, but also audio, video, and still images, as well as interactive, real-time dialogue. Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer. As the District Court found, "the content on the Internet is

as diverse as human thought." We agree with its conclusion that our cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium.

VI

Regardless of whether the CDA is so vague that it violates the Fifth Amendment, the many ambiguities concerning the scope of its coverage render it problematic for purposes of the First Amendment. For instance, each of the two parts of the CDA uses a different linguistic form. The first uses the word "indecent," while the second speaks of material that "in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs." Given the absence of a definition of either term, this difference in language will provoke uncertainty among speakers about how the two standards relate to each other and just what they mean. Could a speaker confidently assume that a serious discussion about birth control practices, homosexuality, the First Amendment issues raised by the Appendix to our *Pacifica* opinion, or the consequences of prison rape would not violate the CDA? This uncertainty undermines the likelihood that the CDA has been carefully tailored to the congressional goal of protecting minors from potentially harmful materials.

The vagueness of the CDA is a matter of special concern for two reasons. First, the CDA is a content-based regulation of speech. The vagueness of such a regulation raises special First Amendment concerns because of its obvious chilling effect on free speech. Second, the CDA is a criminal statute. In addition to the opprobrium and stigma of a criminal conviction, the CDA threatens violators with penalties including up to two years in prison for each act of violation. The severity of criminal sanctions may well cause speakers to remain silent rather than communicate even arguably unlawful words, ideas, and images. As a practical matter, this increased deterrent effect, coupled with the "risk of discriminatory enforcement" of vague regulations, poses greater First Amendment concerns than those implicated by the civil regulation reviewed in Denver Area Ed. Telecommunications Consortium, Inc. v. FCC, 518 U.S. 727 (1996).

The Government argues that the statute is no more vague than the obscenity standard this Court established in Miller v. California, 413 U.S. 15 (1973). But that is not so. In *Miller*, this Court reviewed a criminal conviction against a commercial vendor who mailed brochures containing pictures of sexually explicit activities to individuals who had not requested such materials. Having struggled for some time to establish a definition of obscenity, we set forth in *Miller* the test for obscenity that controls to this day:

> "(a) whether the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value."

Because the CDA's "patently offensive" standard (and, we assume, arguendo, its synonymous "indecent" standard) is one part of the three-prong *Miller* test, the Government reasons, it cannot be unconstitutionally vague.

The Government's assertion is incorrect as a matter of fact. The second prong of the *Miller* test—the purportedly analogous standard—contains a critical requirement that is omitted from the CDA: that the proscribed material be "specifically defined by the applicable state law." This requirement reduces the vagueness inherent in the open-ended term "patently offensive" as used in the CDA. Moreover, the *Miller* definition is limited to "sexual conduct," whereas the CDA extends also to include (1) "excretory activities" as well as (2) "organs" of both a sexual and excretory nature.

The Government's reasoning is also flawed. Just because a definition including three limitations is not vague, it does not follow that one of those limitations, standing by itself, is not vague. Each of *Miller's* additional two prongs—(1) that, taken as a whole, the material appeal to the "prurient" interest, and (2) that it "lac[k] serious literary, artistic, political, or scientific value"—critically limits the uncertain sweep of the obscenity definition. The second requirement is particularly important because, unlike the "patently offensive" and "prurient interest" criteria, it is not judged by contemporary community standards. This "societal value" requirement, absent in the CDA, allows appellate courts to impose some limitations and regularity on the definition by setting, as a matter of law, a national floor for socially redeeming value. The Government's contention that courts will be able to give such legal limitations to the CDA's standards is belied by *Miller's* own rationale for having juries determine whether material is "patently offensive" according to community standards: that such questions are essentially ones of fact.

In contrast to Miller and our other previous cases, the CDA thus presents a greater threat of censoring speech that, in fact, falls outside the statute's scope. Given the vague contours of the coverage of the statute, it unquestionably silences some speakers whose messages would be entitled to constitutional protection. That danger provides further reason for insisting that the statute not be overly broad. The CDA's burden on protected speech cannot be justified if it could be avoided by a more carefully drafted statute.

VII

We are persuaded that the CDA lacks the precision that the First Amendment requires when a statute regulates the content of speech. In order to deny minors access to potentially harmful speech, the CDA effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another. That burden on adult speech is unacceptable if less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve.

In evaluating the free speech rights of adults, we have made it perfectly clear that "[s]exual expression which is indecent but not obscene is protected by the First Amendment." Indeed, *Pacifica* itself admonished that "the fact that society may find speech offensive is not a sufficient reason for suppressing it."

It is true that we have repeatedly recognized the governmental interest in protecting children from harmful materials. But that interest does not justify an unnecessarily broad suppression of speech addressed to adults. As we have explained, the Government may not "reduc[e] the adult

population ... to ... only what is fit for children." "[R]egardless of the strength of the government's interest" in protecting children, "[t]he level of discourse reaching a mailbox simply cannot be limited to that which would be suitable for a sandbox."

The District Court was correct to conclude that the CDA effectively resembles the ban on "dial-a-porn" invalidated in *Sable*. In *Sable*, this Court rejected the argument that we should defer to the congressional judgment that nothing less than a total ban would be effective in preventing enterprising youngsters from gaining access to indecent communications. *Sable* thus made clear that the mere fact that a statutory regulation of speech was enacted for the important purpose of protecting children from exposure to sexually explicit material does not foreclose inquiry into its validity. As we pointed out last Term, that inquiry embodies an "overarching commitment" to make sure that Congress has designed its statute to accomplish its purpose "without imposing an unnecessarily great restriction on speech."

In arguing that the CDA does not so diminish adult communication, the Government relies on the incorrect factual premise that prohibiting a transmission whenever it is known that one of its recipients is a minor would not interfere with adult-to-adult communication. The findings of the District Court make clear that this premise is untenable. Given the size of the potential audience for most messages, in the absence of a viable age verification process, the sender must be charged with knowing that one or more minors will likely view it. Knowledge that, for instance, one or more members of a 100-person chat group will be a minor—and therefore that it would be a crime to send the group an indecent message—would surely burden communication among adults.

The District Court found that at the time of trial existing technology did not include any effective method for a sender to prevent minors from obtaining access to its communications on the Internet without also denying access to adults. The Court found no effective way to determine the age of a user who is accessing material through e-mail, mail exploders, newsgroups, or chat rooms. As a practical matter, the Court also found that it would be prohibitively expensive for noncommercial—as well as some commercial—speakers who have Web sites to verify that their users are adults. These limitations must inevitably curtail a significant amount of adult communication on the Internet. By contrast, the District Court found that "[d]espite its limitations, currently available user-based software suggests that a reasonably effective method by which parents can prevent their children from accessing sexually explicit and other material which *parents* may believe is inappropriate for their children will soon be widely available." (emphases added).

The breadth of the CDA's coverage is wholly unprecedented. Unlike the regulations upheld in *Ginsberg* and *Pacifica*, the scope of the CDA is not limited to commercial speech or commercial entities. Its open-ended prohibitions embrace all nonprofit entities and individuals posting indecent messages or displaying them on their own computers in the presence of minors. The general, undefined terms "indecent" and "patently offensive" cover large amounts of nonpornographic material with serious educational or other value. Moreover, the "community standards" criterion as applied to the Internet means that any communication available to a nation wide audience will be judged by the standards of the community most likely to be offended by the message. The regulated subject matter includes any of the seven "dirty words"

used in the *Pacifica* monologue, the use of which the Government's expert acknowledged could constitute a felony. It may also extend to discussions about prison rape or safe sexual practices, artistic images that include nude subjects, and arguably the card catalog of the Carnegie Library.

For the purposes of our decision, we need neither accept nor reject the Government's submission that the First Amendment does not forbid a blanket prohibition on all "indecent" and "patently offensive" messages communicated to a 17-year-old-no matter how much value the message may contain and regardless of parental approval. It is at least clear that the strength of the Government's interest in protecting minors is not equally strong throughout the coverage of this broad statute. Under the CDA, a parent allowing her 17-year-old to use the family computer to obtain information on the Internet that she, in her parental judgment, deems appropriate could face a lengthy prison term. Similarly, a parent who sent his 17-year-old college freshman information on birth control via e-mail could be incarcerated even though neither he, his child, nor anyone in their home community found the material "indecent" or "patently offensive," if the college town's community thought otherwise.

The breadth of this content-based restriction of speech imposes an especially heavy burden on the Government to explain why a less restrictive provision would not be as effective as the CDA. It has not done so. The arguments in this Court have referred to possible alternatives such as requiring that indecent material be "tagged" in a way that facilitates parental control of material coming into their homes, making exceptions for messages with artistic or educational value, providing some tolerance for parental choice, and regulating some portions of the Internet—such as commercial Web sites—differently from others, such as chat rooms. Particularly in the light of the absence of any detailed findings by the Congress, or even hearings addressing the special problems of the CDA, we are persuaded that the CDA is not narrowly tailored if that requirement has any meaning at all.

VIII

In an attempt to curtail the CDA's facial overbreadth, the Government advances three additional arguments for sustaining the Act's affirmative prohibitions: (1) that the CDA is constitutional because it leaves open ample "alternative channels" of communication; (2) that the plain meaning of the CDA's "knowledge" and "specific person" requirement significantly restricts its permissible applications; and (3) that the CDA's prohibitions are "almost always" limited to material lacking redeeming social value.

The Government first contends that, even though the CDA effectively censors discourse on many of the Internet's modalities—such as chat groups, newsgroups, and mail exploders—it is nonetheless constitutional because it provides a "reasonable opportunity" for speakers to engage in the restricted speech on the World Wide Web. This argument is unpersuasive because the CDA regulates speech on the basis of its content. A "time, place, and manner" analysis is therefore inapplicable. It is thus immaterial whether such speech would be feasible on the Web (which, as the Government's own expert acknowledged, would cost up to $10,000 if the speaker's interests were not accommodated by an existing Web site, not including costs for data base management and age verification). The Government's position is equivalent to arguing that a statute could ban leaflets on certain subjects as long as individuals are free to publish books. In

invalidating a number of laws that banned leafletting on the streets regardless of their content, we explained that "one is not to have the exercise of his liberty of expression in appropriate places abridged on the plea that it may be exercised in some other place."

The Government also asserts that the "knowledge" requirement of both §§ 223(a) and (d), especially when coupled with the "specific child" element found in § 223(d), saves the CDA from overbreadth. Because both sections prohibit the dissemination of indecent messages only to persons known to be under 18, the Government argues, it does not require transmitters to "refrain from communicating indecent material to adults; they need only refrain from disseminating such materials to persons they know to be under 18." This argument ignores the fact that most Internet forums—including chat rooms, newsgroups, mail exploders, and the Web—are open to all comers. The Government's assertion that the knowledge requirement somehow protects the communications of adults is therefore untenable. Even the strongest reading of the "specific person" requirement of § 223(d) cannot save the statute. It would confer broad powers of censorship, in the form of a "heckler's veto," upon any opponent of indecent speech who might simply log on and inform the would-be discoursers that his 17-year-old child—a "specific person ... under 18 years of age"—would be present.

Finally, we find no textual support for the Government's submission that material having scientific, educational, or other redeeming social value will necessarily fall outside the CDA's "patently offensive" and "indecent" prohibitions.

IX

The Government's three remaining arguments focus on the defenses provided in § 223(e)(5). First, relying on the "good faith, reasonable, effective, and appropriate actions" provision, the Government suggests that "tagging" provides a defense that saves the constitutionality of the CDA. The suggestion assumes that transmitters may encode their indecent communications in a way that would indicate their contents, thus permitting recipients to block their reception with appropriate software. It is the requirement that the good-faith action must be "effective" that makes this defense illusory. The Government recognizes that its proposed screening software does not currently exist. Even if it did, there is no way to know whether a potential recipient will actually block the encoded material. Without the impossible knowledge that every guardian in America is screening for the "tag," the transmitter could not reasonably rely on its action to be "effective."

For its second and third arguments concerning defenses—which we can consider together—the Government relies on the latter half of § 223(e)(5), which applies when the transmitter has restricted access by requiring use of a verified credit card or adult identification. Such verification is not only technologically available but actually is used by commercial providers of sexually explicit material. These providers, therefore, would be protected by the defense. Under the findings of the District Court, however, it is not economically feasible for most noncommercial speakers to employ such verification. Accordingly, this defense would not significantly narrow the statute's burden on noncommercial speech. Even with respect to the commercial pornographers that would be protected by the defense, the Government failed to adduce any evidence that these verification techniques actually preclude minors from posing as

adults. Given that the risk of criminal sanctions "hovers over each content provider, like the proverbial sword of Damocles," the District Court correctly refused to rely on unproven future technology to save the statute. The Government thus failed to prove that the proffered defense would significantly reduce the heavy burden on adult speech produced by the prohibition on offensive displays.

We agree with the District Court's conclusion that the CDA places an unacceptably heavy burden on protected speech, and that the defenses do not constitute the sort of "narrow tailoring" that will save an otherwise patently invalid unconstitutional provision. In *Sable*, 492 U.S., at 127, we remarked that the speech restriction at issue there amounted to "'burn[ing] the house to roast the pig.'" The CDA, casting a far darker shadow over free speech, threatens to torch a large segment of the Internet community.

X

At oral argument, the Government relied heavily on its ultimate fall-back position: If this Court should conclude that the CDA is insufficiently tailored, it urged, we should save the statute's constitutionality by honoring the severability clause, and construing nonseverable terms narrowly. In only one respect is this argument acceptable.

A severability clause requires textual provisions that can be severed. We will follow § 608's guidance by leaving constitutional textual elements of the statute intact in the one place where they are, in fact, severable. The "indecency" provision, applies to "any comment, request, suggestion, proposal, image, or other communication which is *obscene or indecent*." (Emphasis added.) Appellees do not challenge the application of the statute to obscene speech, which, they acknowledge, can be banned totally because it enjoys no First Amendment protection. As set forth by the statute, the restriction of "obscene" material enjoys a textual manifestation separate from that for "indecent" material, which we have held unconstitutional. Therefore, we will sever the term "or indecent" from the statute, leaving the rest of § 223(a) standing. In no other respect, however, can § 223(a) or § 223(d) be saved by such a textual surgery.

The Government also draws on an additional, less traditional aspect of the CDA's severability clause, which asks any reviewing court that holds the statute facially unconstitutional not to invalidate the CDA in application to "other persons or circumstances" that might be constitutionally permissible. It further invokes this Court's admonition that, absent "countervailing considerations," a statute should "be declared invalid to the extent it reaches too far, but otherwise left intact." There are two flaws in this argument.

First, the statute that grants our jurisdiction for this expedited review, limits that jurisdictional grant to actions challenging the CDA "on its face." Consistent with § 561, the plaintiffs who brought this suit and the three-judge panel that decided it treated it as a facial challenge. We have no authority, in this particular posture, to convert this litigation into an "as-applied" challenge. Nor, given the vast array of plaintiffs, the range of their expressive activities, and the vagueness of the statute, would it be practicable to limit our holding to a judicially defined set of specific applications.

Second, one of the "countervailing considerations" mentioned in *Brockett* is present here. In considering a facial challenge, this Court may impose a limiting construction on a statute only if it is "readily susceptible" to such a construction. The open-ended character of the CDA provides no guidance what ever for limiting its coverage….

XI

In this Court, though not in the District Court, the Government asserts that—in addition to its interest in protecting children—its "[e]qually significant" interest in fostering the growth of the Internet provides an independent basis for upholding the constitutionality of the CDA. The Government apparently assumes that the unregulated availability of "indecent" and "patently offensive" material on the Internet is driving countless citizens away from the medium because of the risk of exposing themselves or their children to harmful material.

We find this argument singularly unpersuasive. The dramatic expansion of this new marketplace of ideas contradicts the factual basis of this contention. The record demonstrates that the growth of the Internet has been and continues to be phenomenal. As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship.

For the foregoing reasons, the judgment of the District Court is affirmed.

Justice O'CONNOR, with whom THE CHIEF JUSTICE joins, concurring in the judgment in part and dissenting in part.

I write separately to explain why I view the Communications Decency Act of 1996 (CDA) as little more than an attempt by Congress to create "adult zones" on the Internet. Our precedent indicates that the creation of such zones can be constitutionally sound. Despite the soundness of its purpose, however, portions of the CDA are unconstitutional because they stray from the blueprint our prior cases have developed for constructing a "zoning law" that passes constitutional muster.

Appellees bring a facial challenge to three provisions of the CDA. The first, which the Court describes as the "indecency transmission" provision, makes it a crime to knowingly transmit an obscene or indecent message or image to a person the sender knows is under 18 years old. What the Court classifies as a single "'patently offensive display'" provision is in reality two separate provisions. The first of these makes it a crime to knowingly send a patently offensive message or image to a specific person under the age of 18 ("specific person" provision). The second criminalizes the display of patently offensive messages or images "in a[ny] manner available" to minors ("display" provision). None of these provisions purports to keep indecent (or patently offensive) material away from adults, who have a First Amendment right to obtain this speech. Thus, the undeniable purpose of the CDA is to segregate indecent material on the Internet into certain areas that minors cannot access. See S. Conf. Rep. No. 104-230, p. 189 (1996) (CDA imposes "access restrictions ... to protect minors from exposure to indecent material").

The creation of "adult zones" is by no means a novel concept. States have long denied minors access to certain establishments frequented by adults. States have also denied minors access to speech deemed to be "harmful to minors." The Court has previously sustained such zoning laws, but only if they respect the First Amendment rights of adults and minors. That is to say, a zoning law is valid if (i) it does not unduly restrict adult access to the material; and (ii) minors have no First Amendment right to read or view the banned material. As applied to the Internet as it exists in 1997, the "display" provision and some applications of the "indecency transmission" and "specific person" provisions fail to adhere to the first of these limiting principles by restricting adults' access to protected materials in certain circumstances. Unlike the Court, however, I would invalidate the provisions only in those circumstances.

I

Our cases make clear that a "zoning" law is valid only if adults are still able to obtain the regulated speech. If they cannot, the law does more than simply keep children away from speech they have no right to obtain-it interferes with the rights of adults to obtain constitutionally protected speech and effectively "reduce[s] the adult population ... to reading only what is fit for children." The First Amendment does not tolerate such interference. If the law does not unduly restrict adults' access to constitutionally protected speech, however, it may be valid. In Ginsberg v. New York, 390 U.S. 629, 634 (1968), for example, the Court sustained a New York law that barred store owners from selling pornographic magazines to minors in part because adults could still buy those magazines.

The Court in *Ginsberg* concluded that the New York law created a constitutionally adequate adult zone simply because, on its face, it denied access only to minors. The Court did not question—and therefore necessarily assumed—that an adult zone, once created, would succeed in preserving adults' access while denying minors' access to the regulated speech. Before today, there was no reason to question this assumption, for the Court has previously only considered laws that operated in the physical world, a world that with two characteristics that make it possible to create "adult zones": geography and identity. A minor can see an adult dance show only if he enters an establishment that provides such entertainment. And should he attempt to do so, the minor will not be able to conceal completely his identity (or, consequently, his age). Thus, the twin characteristics of geography and identity enable the establishment's proprietor to prevent children from entering the establishment, but to let adults inside.

The electronic world is fundamentally different. Because it is no more than the interconnection of electronic pathways, cyberspace allows speakers and listeners to mask their identities. Cyberspace undeniably reflects some form of geography; chat rooms and Web sites, for example, exist at fixed "locations" on the Internet. Since users can transmit and receive messages on the Internet without revealing anything about their identities or ages, however, it is not currently possible to exclude persons from accessing certain messages on the basis of their identity.

Cyberspace differs from the physical world in another basic way: Cyberspace is malleable. Thus, it is possible to construct barriers in cyberspace and use them to screen for identity, making

cyberspace more like the physical world and, consequently, more amenable to zoning laws. This transformation of cyberspace is already underway. Internet speakers (users who post material on the Internet) have begun to zone cyberspace itself through the use of "gateway" technology. Such technology requires Internet users to enter information about themselves—perhaps an adult identification number or a credit card number—before they can access certain areas of cyberspace, much like a bouncer checks a person's driver's license before admitting him to a nightclub. Internet users who access information have not attempted to zone cyberspace itself, but have tried to limit their own power to access information in cyberspace, much as a parent controls what her children watch on television by installing a lock box. This user-based zoning is accomplished through the use of screening software (such as Cyber Patrol or SurfWatch) or browsers with screening capabilities, both of which search addresses and text for keywords that are associated with "adult" sites and, if the user wishes, blocks access to such sites. The Platform for Internet Content Selection project is designed to facilitate user-based zoning by encouraging Internet speakers to rate the content of their speech using codes recognized by all screening programs.

Despite this progress, the transformation of cyberspace is not complete. Although gateway technology has been available on the World Wide Web for some time now, it is not available to all Web speakers, and is just now becoming technologically feasible for chat rooms and USENET newsgroups. Gateway technology is not ubiquitous in cyberspace, and because without it "there is no means of age verification," cyberspace still remains largely unzoned—and unzoneable. User-based zoning is also in its infancy. For it to be effective, (i) an agreed-upon code (or "tag") would have to exist; (ii) screening software or browsers with screening capabilities would have to be able to recognize the "tag"; and (iii) those programs would have to be widely available-and widely used-by Internet users. At present, none of these conditions is true. Screening software "is not in wide use today" and "only a handful of browsers have screening capabilities." There is, moreover, no agreed-upon "tag" for those programs to recognize.

Although the prospects for the eventual zoning of the Internet appear promising, I agree with the Court that we must evaluate the constitutionality of the CDA as it applies to the Internet as it exists today. Given the present state of cyberspace, I agree with the Court that the "display" provision cannot pass muster. Until gateway technology is available throughout cyberspace, and it is not in 1997, a speaker cannot be reasonably assured that the speech he displays will reach only adults because it is impossible to confine speech to an "adult zone." Thus, the only way for a speaker to avoid liability under the CDA is to refrain completely from using indecent speech. But this forced silence impinges on the First Amendment right of adults to make and obtain this speech and, for all intents and purposes, "reduce[s] the adult population [on the Internet] to reading only what is fit for children." As a result, the "display" provision cannot withstand scrutiny.

The "indecency transmission" and "specific person" provisions present a closer issue, for they are not unconstitutional in all of their applications. As discussed above, the "indecency transmission" provision makes it a crime to transmit knowingly an indecent message to a person the sender knows is under 18 years of age. The "specific person" provision proscribes the same conduct, although it does not as explicitly require the sender to know that the intended recipient

of his indecent message is a minor. The Government urges the Court to construe the provision to impose such a knowledge requirement, and I would do so.

So construed, both provisions are constitutional as applied to a conversation involving only an adult and one or more minors—e.g., when an adult speaker sends an e-mail knowing the addressee is a minor, or when an adult and minor converse by themselves or with other minors in a chat room. In this context, these provisions are no different from the law we sustained in *Ginsberg*. Restricting what the adult may say to the minors in no way restricts the adult's ability to communicate with other adults. He is not prevented from speaking indecently to other adults in a chat room (because there are no other adults participating in the conversation) and he remains free to send indecent e-mails to other adults. The relevant universe contains only one adult, and the adult in that universe has the power to refrain from using indecent speech and consequently to keep all such speech within the room in an "adult" zone.

The analogy to *Ginsberg* breaks down, however, when more than one adult is a party to the conversation. If a minor enters a chat room otherwise occupied by adults, the CDA effectively requires the adults in the room to stop using indecent speech. If they did not, they could be prosecuted under the "indecency transmission" and "specific person" provisions for any indecent statements they make to the group, since they would be transmitting an indecent message to specific persons, one of whom is a minor. The CDA is therefore akin to a law that makes it a crime for a bookstore owner to sell pornographic magazines to anyone once a minor enters his store. Even assuming such a law might be constitutional in the physical world as a reasonable alternative to excluding minors completely from the store, the absence of any means of excluding minors from chat rooms in cyberspace restricts the rights of adults to engage in indecent speech in those rooms. The "indecency transmission" and "specific person" provisions share this defect.

But these two provisions do not infringe on adults' speech in all situations. And as discussed below, I do not find that the provisions are overbroad in the sense that they restrict minors' access to a substantial amount of speech that minors have the right to read and view. Accordingly, the CDA can be applied constitutionally in some situations. Normally, this fact would require the Court to reject a direct facial challenge. Appellees' claim arises under the First Amendment, however, and they argue that the CDA is facially invalid because it is "substantially overbroad"—that is, it "sweeps too broadly ... [and] penaliz[es] a substantial amount of speech that is constitutionally protected." I agree with the Court that the provisions are overbroad in that they cover any and all communications between adults and minors, regardless of how many adults might be part of the audience to the communication.

This conclusion does not end the matter, however. Where, as here, "the parties challenging the statute are those who desire to engage in protected speech that the overbroad statute purports to punish, ... [t]he statute may forthwith be declared invalid to the extent that it reaches too far, but otherwise left intact." There is no question that Congress intended to prohibit certain communications between one adult and one or more minors. There is also no question that Congress would have enacted a narrower version of these provisions had it known a broader version would be declared unconstitutional. I would therefore sustain the "indecency transmission" and "specific person" provisions to the extent they apply to the transmission of

Internet communications where the party initiating the communication knows that all of the recipients are minors.

II

Whether the CDA substantially interferes with the First Amendment rights of minors, and thereby runs afoul of the second characteristic of valid zoning laws, presents a closer question. In *Ginsberg*, the New York law we sustained prohibited the sale to minors of magazines that were "harmful to minors." Under that law, a magazine was "harmful to minors" only if it was obscene as to minors. Noting that obscene speech is not protected by the First Amendment, and that New York was constitutionally free to adjust the definition of obscenity for minors, the Court concluded that the law did not "invad[e] the area of freedom of expression constitutionally secured to minors." New York therefore did not infringe upon the First Amendment rights of minors.

The Court neither "accept[s] nor reject[s]" the argument that the CDA is facially overbroad because it substantially interferes with the First Amendment rights of minors. I would reject it. *Ginsberg* established that minors may constitutionally be denied access to material that is obscene as to minors. As *Ginsberg* explained, material is obscene as to minors if it (i) is "patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable ... for minors"; (ii) appeals to the prurient interest of minors; and (iii) is "utterly without redeeming social importance for minors." Because the CDA denies minors the right to obtain material that is "patently offensive"—even if it has some redeeming value for minors and even if it does not appeal to their prurient interests—Congress' rejection of the *Ginsberg* "harmful to minors" standard means that the CDA could ban some speech that is "indecent" (i.e., "patently offensive") but that is not obscene as to minors.

I do not deny this possibility, but to prevail in a facial challenge, it is not enough for a plaintiff to show "some" overbreadth. Our cases require a proof of "real" and "substantial" overbreadth, and appellees have not carried their burden in this case. In my view, the universe of speech constitutionally protected as to minors but banned by the CDA—i.e., the universe of material that is "patently offensive," but which nonetheless has some redeeming value for minors or does not appeal to their prurient interest—is a very small one. Appellees cite no examples of speech falling within this universe and do not attempt to explain why that universe is substantial "in relation to the statute's plainly legitimate sweep." That the CDA might deny minors the right to obtain material that has some "value" is largely beside the point. While discussions about prison rape or nude art may have some redeeming educational value for adults, they do not necessarily have any such value for minors, and under *Ginsberg*, minors only have a First Amendment right to obtain patently offensive material that has "redeeming social importance *for minors*." There is also no evidence in the record to support the contention that "many e-mail transmissions from an adult to a minor are conversations between family members," and no support for the legal proposition that such speech is absolutely immune from regulation. Accordingly, in my view, the CDA does not burden a substantial amount of minors' constitutionally protected speech.

Thus, the constitutionality of the CDA as a zoning law hinges on the extent to which it substantially interferes with the First Amendment rights of adults. Because the rights of adults

are infringed only by the "display" provision and by the "indecency transmission" and "specific person" provisions as applied to communications involving more than one adult, I would invalidate the CDA only to that extent. Insofar as the "indecency transmission" and "specific person" provisions prohibit the use of indecent speech in communications between an adult and one or more minors, however, they can and should be sustained. The Court reaches a contrary conclusion, and from that holding that I respectfully dissent.

Ashcroft v. American Civil Liberties Union, 542 U.S. 656 (2004).
Kennedy, Justice.

This case presents a challenge to a statute enacted by Congress to protect minors from exposure to sexually explicit materials on the Internet, the Child Online Protection Act (COPA). We must decide whether the Court of Appeals was correct to affirm a ruling by the District Court that enforcement of COPA should be enjoined because the statute likely violates the First Amendment.

In enacting COPA, Congress gave consideration to our earlier decisions on this subject, in particular the decision in Reno v. American Civil Liberties Union, 521 U.S. 844 (1997). For that reason, "the Judiciary must proceed with caution and ... with care before invalidating the Act." The imperative of according respect to the Congress, however, does not permit us to depart from well-established First Amendment principles. Instead, we must hold the Government to its constitutional burden of proof.

Content-based prohibitions, enforced by severe criminal penalties, have the constant potential to be a repressive force in the lives and thoughts of a free people. To guard against that threat the Constitution demands that content-based restrictions on speech be presumed invalid, Rand that the Government bear the burden of showing their constitutionality. This is true even when Congress twice has attempted to find a constitutional means to restrict, and punish, the speech in question….

I
A

COPA is the second attempt by Congress to make the Internet safe for minors by criminalizing certain Internet speech. The first attempt was the Communications Decency Act of 1996. The Court held the CDA unconstitutional because it was not narrowly tailored to serve a compelling governmental interest and because less restrictive alternatives were available.

In response to the Court's decision in *Reno*, Congress passed COPA. COPA imposes criminal penalties of a $50,000 fine and six months in prison for the knowing posting, for "commercial purposes," of World Wide Web content that is "harmful to minors." Material that is "harmful to minors" is defined as:

> "any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that is obscene or that-
>
> "(A) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest;
>
> "(B) depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or

> simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and
>
> "(C) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors."

"Minor[s]" are defined as "any person under 17 years of age." A person acts for "commercial purposes only if such person is engaged in the business of making such communications." "Engaged in the business," in turn,

> "means that the person who makes a communication, or offers to make a communication, by means of the World Wide Web, that includes any material that is harmful to minors, devotes time, attention, or labor to such activities, as a regular course of such person's trade or business, with the objective of earning a profit as a result of such activities (although it is not necessary that the person make a profit or that the making or offering to make such communications be the person's sole or principal business or source of income)."

While the statute labels all speech that falls within these definitions as criminal speech, it also provides an affirmative defense to those who employ specified means to prevent minors from gaining access to the prohibited materials on their Web site. A person may escape conviction under the statute by demonstrating that he

> "has restricted access by minors to material that is harmful to minors-
>
> "(A) by requiring use of a credit card, debit account, adult access code, or adult personal identification number;
>
> "(B) by accepting a digital certificate that verifies age; or
>
> "(C) by any other reasonable measures that are feasible under available technology."

Since the passage of COPA, Congress has enacted additional laws regulating the Internet in an attempt to protect minors. For example, it has enacted a prohibition on misleading Internet domain names, 18 U.S.C. § 2252B, in order to prevent Web site owners from disguising pornographic Web sites in a way likely to cause uninterested persons to visit them. It has also passed a statute creating a "Dot Kids" second-level Internet domain, the content of which is restricted to that which is fit for minors under the age of 13.

B

Respondents, Internet content providers and others concerned with protecting the freedom of speech, filed suit in the United States District Court for the Eastern District of Pennsylvania. They sought a preliminary injunction against enforcement of the statute. After considering

testimony from witnesses presented by both respondents and the Government, the District Court issued an order granting the preliminary injunction….

The Government appealed the District Court's decision to the United States Court of Appeals for the Third Circuit. The Court of Appeals affirmed the preliminary injunction, but on a different ground. The court concluded that the "community standards" language in COPA by itself rendered the statute unconstitutionally overbroad. We granted certiorari and reversed, holding that the community-standards language did not, standing alone, make the statute unconstitutionally overbroad. We emphasized, however, that our decision was limited to that narrow issue. We remanded the case to the Court of Appeals to reconsider whether the District Court had been correct to grant the preliminary injunction. On remand, the Court of Appeals again affirmed the District Court….

II

A…

The District Court, in deciding to grant the preliminary injunction, concentrated primarily on the argument that there are plausible, less restrictive alternatives to COPA. A statute that "effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another ... is unacceptable if less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve." When plaintiffs challenge a content-based speech restriction, the burden is on the Government to prove that the proposed alternatives will not be as effective as the challenged statute.

In considering this question, a court assumes that certain protected speech may be regulated, and then asks what is the least restrictive alternative that can be used to achieve that goal. The purpose of the test is not to consider whether the challenged restriction has some effect in achieving Congress' goal, regardless of the restriction it imposes. The purpose of the test is to ensure that speech is restricted no further than necessary to achieve the goal, for it is important to ensure that legitimate speech is not chilled or punished. For that reason, the test does not begin with the status quo of existing regulations, then ask whether the challenged restriction has some additional ability to achieve Congress' legitimate interest. Any restriction on speech could be justified under that analysis. Instead, the court should ask whether the challenged regulation is the least restrictive means among available, effective alternatives.

…As the Government bears the burden of proof on the ultimate question of COPA's constitutionality, respondents must be deemed likely to prevail unless the Government has shown that respondents' proposed less restrictive alternatives are less effective than COPA. Applying that analysis, the District Court concluded that respondents were likely to prevail. That conclusion was not an abuse of discretion, because on this record there are a number of plausible, less restrictive alternatives to the statute.

The primary alternative considered by the District Court was blocking and filtering software. Blocking and filtering software is an alternative that is less restrictive than COPA, and, in addition, likely more effective as a means of restricting children's access to materials harmful to them. The District Court, in granting the preliminary injunction, did so primarily because the

plaintiffs had proposed that filters are a less restrictive alternative to COPA and the Government had not shown it would be likely to disprove the plaintiffs' contention at trial.

Filters are less restrictive than COPA. They impose selective restrictions on speech at the receiving end, not universal restrictions at the source. Under a filtering regime, adults without children may gain access to speech they have a right to see without having to identify themselves or provide their credit card information. Even adults with children may obtain access to the same speech on the same terms simply by turning off the filter on their home computers. Above all, promoting the use of filters does not condemn as criminal any category of speech, and so the potential chilling effect is eliminated, or at least much diminished. All of these things are true, moreover, regardless of how broadly or narrowly the definitions in COPA are construed.

Filters also may well be more effective than COPA. First, a filter can prevent minors from seeing all pornography, not just pornography posted to the Web from America. The District Court noted in its factfindings that one witness estimated that 40% of harmful-to-minors content comes from overseas. COPA does not prevent minors from having access to those foreign harmful materials. That alone makes it possible that filtering software might be more effective in serving Congress' goals. Effectiveness is likely to diminish even further if COPA is upheld, because the providers of the materials that would be covered by the statute simply can move their operations overseas. It is not an answer to say that COPA reaches some amount of materials that are harmful to minors; the question is whether it would reach more of them than less restrictive alternatives. In addition, the District Court found that verification systems may be subject to evasion and circumvention, for example, by minors who have their own credit cards. Finally, filters also may be more effective because they can be applied to all forms of Internet communication, including e-mail, not just communications available via the World Wide Web.

That filtering software may well be more effective than COPA is confirmed by the findings of the Commission on Child Online Protection, a blue-ribbon Commission created by Congress in COPA itself. Congress directed the Commission to evaluate the relative merits of different means of restricting minors' ability to gain access to harmful materials on the Internet. It unambiguously found that filters are more effective than age-verification requirements. See Commission on Child Online Protection (COPA), Report to Congress, 19-21, 23-25, 27 (Oct. 20, 2000) (assigning a score for "Effectiveness" of 7.4 for server-based filters and 6.5 for client-based filters, as compared to 5.9 for independent adult-ID verification, and 5.5 for credit card verification). Thus, not only has the Government failed to carry its burden of showing the District Court that the proposed alternative is less effective, but also a Government Commission appointed to consider the question has concluded just the opposite. That finding supports our conclusion that the District Court did not abuse its discretion in enjoining the statute.

Filtering software, of course, is not a perfect solution to the problem of children gaining access to harmful-to-minors materials. It may block some materials that are not harmful to minors and fail to catch some that are. Whatever the deficiencies of filters, however, the Government failed to introduce specific evidence proving that existing technologies are less effective than the restrictions in COPA. The District Court made a specific factfinding that "[n]o evidence was presented to the Court as to the percentage of time that blocking and filtering technology is over- or underinclusive." In the absence of a showing as to the relative effectiveness of COPA and the

alternatives proposed by respondents, it was not an abuse of discretion for the District Court to grant the preliminary injunction. The Government's burden is not merely to show that a proposed less restrictive alternative has some flaws; its burden is to show that it is less effective. It is not enough for the Government to show that COPA has some effect. Nor do respondents bear a burden to introduce, or offer to introduce, evidence that their proposed alternatives are more effective. The Government has the burden to show they are less so. The Government having failed to carry its burden, it was not an abuse of discretion for the District Court to grant the preliminary injunction.

One argument to the contrary is worth mentioning—the argument that filtering software is not an available alternative because Congress may not require it to be used. That argument carries little weight, because Congress undoubtedly may act to encourage the use of filters. We have held that Congress can give strong incentives to schools and libraries to use them. United States v. American Library Assn., Inc., 539 U.S. 194 (2003). It could also take steps to promote their development by industry, and their use by parents. It is incorrect, for that reason, to say that filters are part of the current regulatory status quo. The need for parental cooperation does not automatically disqualify a proposed less restrictive alternative. In enacting COPA, Congress said its goal was to prevent the "widespread availability of the Internet" from providing "opportunities for minors to access materials through the World Wide Web in a manner that can frustrate parental supervision or control." COPA presumes that parents lack the ability, not the will, to monitor what their children see. By enacting programs to promote use of filtering software, Congress could give parents that ability without subjecting protected speech to severe penalties….

B

There are also important practical reasons to let the injunction stand pending a full trial on the merits. First, the potential harms from reversing the injunction outweigh those of leaving it in place by mistake. Where a prosecution is a likely possibility, yet only an affirmative defense is available, speakers may self-censor rather than risk the perils of trial. There is a potential for extraordinary harm and a serious chill upon protected speech. The harm done from letting the injunction stand pending a trial on the merits, in contrast, will not be extensive. No prosecutions have yet been undertaken under the law, so none will be disrupted if the injunction stands. Further, if the injunction is upheld, the Government in the interim can enforce obscenity laws already on the books.

Second, there are substantial factual disputes remaining in the case. As mentioned above, there is a serious gap in the evidence as to the effectiveness of filtering software. For us to assume, without proof, that filters are less effective than COPA would usurp the District Court's factfinding role. By allowing the preliminary injunction to stand and remanding for trial, we require the Government to shoulder its full constitutional burden of proof respecting the less restrictive alternative argument, rather than excuse it from doing so.

Third, and on a related point, the factual record does not reflect current technological reality—a serious flaw in any case involving the Internet. The technology of the Internet evolves at a rapid pace. Yet the factfindings of the District Court were entered in February 1999, over five years

ago. Since then, certain facts about the Internet are known to have changed. It is reasonable to assume that other technological developments important to the First Amendment analysis have also occurred during that time. More and better filtering alternatives may exist than when the District Court entered its findings. Indeed, we know that after the District Court entered its factfindings, a congressionally appointed commission issued a report that found that filters are more effective than verification screens.

Delay between the time that a district court makes factfindings and the time that a case reaches this Court is inevitable, with the necessary consequence that there will be some discrepancy between the facts as found and the facts at the time the appellate court takes up the question. We do not mean, therefore, to set up an insuperable obstacle to fair review. Here, however, the usual gap has doubled because the case has been through the Court of Appeals twice. The additional two years might make a difference. By affirming the preliminary injunction and remanding for trial, we allow the parties to update and supplement the factual record to reflect current technological realities.

Remand will also permit the District Court to take account of a changed legal landscape. Since the District Court made its factfindings, Congress has passed at least two further statutes that might qualify as less restrictive alternatives to COPA—a prohibition on misleading domain names, and a statute creating a minors-safe "Dot Kids" domain. Remanding for trial will allow the District Court to take into account those additional potential alternatives.

On a final point, it is important to note that this opinion does not hold that Congress is incapable of enacting any regulation of the Internet designed to prevent minors from gaining access to harmful materials. The parties, because of the conclusion of the Court of Appeals that the statute's definitions rendered it unconstitutional, did not devote their attention to the question whether further evidence might be introduced on the relative restrictiveness and effectiveness of alternatives to the statute. On remand, however, the parties will be able to introduce further evidence on this point. This opinion does not foreclose the District Court from concluding, upon a proper showing by the Government that meets the Government's constitutional burden as defined in this opinion, that COPA is the least restrictive alternative available to accomplish Congress' goal….

[Justice Stevens' concurrence and Justice Scalia's dissent omitted].

Justice BREYER, with whom THE CHIEF JUSTICE and Justice O'CONNOR join, dissenting.

The Child Online Protection Act (Act) seeks to protect children from exposure to commercial pornography placed on the Internet. It does so by requiring commercial providers to place pornographic material behind Internet "screens" readily accessible to adults who produce age verification. The Court recognizes that we should "'proceed ... with care before invalidating the Act,'" while pointing out that the "imperative of according respect to the Congress ... does not permit us to depart from well-established First Amendment principles." I agree with these generalities. Like the Court, I would subject the Act to "the most exacting scrutiny," requiring the Government to show that any restriction of nonobscene expression is "narrowly drawn" to

further a "compelling interest" and that the restriction amounts to the "least restrictive means" available to further that interest.

Nonetheless, my examination of (1) the burdens the Act imposes on protected expression, (2) the Act's ability to further a compelling interest, and (3) the proposed "less restrictive alternatives" convinces me that the Court is wrong. I cannot accept its conclusion that Congress could have accomplished its statutory objective—protecting children from commercial pornography on the Internet—in other, less restrictive ways.

I

Although the Court rests its conclusion upon the existence of less restrictive alternatives, I must first examine the burdens that the Act imposes upon protected speech. That is because the term "less restrictive alternative" is a comparative term. An "alternative" is "less restrictive" only if it will work less First Amendment harm than the statute itself, while at the same time similarly furthering the "compelling" interest that prompted Congress to enact the statute. Unlike the majority, I do not see how it is possible to make this comparative determination without examining both the extent to which the Act regulates protected expression and the nature of the burdens it imposes on that expression. That examination suggests that the Act, properly interpreted, imposes a burden on protected speech that is no more than modest.

A

The Act's definitions limit the material it regulates to material that does not enjoy First Amendment protection, namely, legally obscene material, and very little more. A comparison of this Court's definition of unprotected, "legally obscene," material with the Act's definitions makes this clear.

Material is legally obscene if

> "(a) ... 'the average person, applying contemporary community standards' would find that the work, taken as a whole, appeals to the prurient interest ...; (b) ... the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) ... the work, taken as a whole, lacks serious literary, artistic, political, or scientific value."

The present statute defines the material that it regulates as material that meets all of the following criteria:

> "(A) the average person, applying contemporary community standards, would find, taking the material as a whole *and with respect to minors*, [that the material] is designed to appeal to, or is designed to pander to, the prurient interest;
>
> "(B) [the material] depicts, describes, or represents, in a manner patently offensive *with respect to minors*, an actual or simulated sexual act or sexual

> contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and
>
> "(C) [the material] taken as a whole, lacks serious literary, artistic, political, or scientific value *for minors*." (emphasis added).

Both definitions define the relevant material through use of the critical terms "prurient interest" and "lacks serious literary, artistic, political, or scientific value." Insofar as material appeals to, or panders to, "the prurient interest," it simply seeks a sexual response. Insofar as "patently offensive" material with "no serious value" simply seeks that response, it does not seek to educate, it does not seek to elucidate views about sex, it is not artistic, and it is not literary. That is why this Court, in *Miller*, held that the First Amendment did not protect material that fit its definition.

The only significant difference between the present statute and *Miller's* definition consists of the addition of the words "with respect to minors" and "for minors." But the addition of these words to a definition that would otherwise cover only obscenity expands the statute's scope only slightly. That is because the material in question (while potentially harmful to young children) must, first, appeal to the "prurient interest" of, i.e., seek a sexual response from, some group of adolescents or postadolescents (since young children normally do not so respond). And material that appeals to the "prurient interest[s]" of some group of adolescents or postadolescents will almost inevitably appeal to the "prurient interest[s]" of some group of adults as well.

The "lack of serious value" requirement narrows the statute yet further—despite the presence of the qualification "for minors." That is because one cannot easily imagine material that has serious literary, artistic, political, or scientific value for a significant group of adults, but lacks such value for any significant group of minors. Thus, the statute, read literally, insofar as it extends beyond the legally obscene, could reach only borderline cases. And to take the words of the statute literally is consistent with Congress' avowed objective in enacting this law; namely, putting material produced by professional pornographers behind screens that will verify the age of the viewer. See S.Rep. No. 105-225, p. 3 (1998) (hereinafter S. Rep.) ("The bill seeks to restrict access to commercial pornography on the Web by requiring those engaged in the business of the commercial distribution of material that is harmful to minors to take certain prescribed steps to restrict access to such material by minors ..."); H.R.Rep. No. 105-775, pp. 5, 14 (1998) (hereinafter H.R. Rep.) (explaining that the bill is aimed at the sale of pornographic materials and provides a defense for the "commercial purveyors of pornography" that the bill seeks to regulate).

These limitations on the statute's scope answer many of the concerns raised by those who attack its constitutionality. Respondents fear prosecution for the Internet posting of material that does not fall within the statute's ambit as limited by the "prurient interest" and "no serious value" requirements; for example: an essay about a young man's experience with masturbation and sexual shame; "a serious discussion about birth control practices, homosexuality, ... or the consequences of prison rape"; an account by a 15-year-old, written for therapeutic purposes, of being raped when she was 13; a guide to self-examination for testicular cancer; a graphic illustration of how to use a condom; or any of the other postings of modern literary or artistic

works or discussions of sexual identity, homosexuality, sexually transmitted diseases, sex education, or safe sex, let alone Aldous Huxley's Brave New World, J.D. Salinger's Catcher in the Rye, or, as the complaint would have it, "Ken Starr's report on the Clinton-Lewinsky scandal."

These materials are not both (1) "designed to appeal to, or ... pander to, the prurient interest" of significant groups of minors and (2) lacking in "serious literary, artistic, political, or scientific value" for significant groups of minors. Thus, they fall outside the statute's definition of the material that it restricts, a fact the Government acknowledged at oral argument.

I have found nothing elsewhere in the statute's language that broadens its scope. Other qualifying phrases, such as "taking the material as a whole," and "for commercial purposes," limit the statute's scope still more, requiring, for example, that individual images be considered in context. In sum, the Act's definitions limit the statute's scope to commercial pornography. It affects unprotected obscene material. Given the inevitable uncertainty about how to characterize close-to-obscene material, it could apply to (or chill the production of) a limited class of borderline material that courts might ultimately find is protected. But the examples I have just given fall outside that class.

B

The Act does not censor the material it covers. Rather, it requires providers of the "harmful to minors" material to restrict minors' access to it by verifying age. They can do so by inserting screens that verify age using a credit card, adult personal identification number, or other similar technology. In this way, the Act requires creation of an Internet screen that minors, but not adults, will find difficult to bypass.

I recognize that the screening requirement imposes some burden on adults who seek access to the regulated material, as well as on its providers. The cost is, in part, monetary. The parties agreed that a Web site could store card numbers or passwords at between 15 and 20 cents per number. And verification services provide free verification to Web site operators, while charging users less than $20 per year. According to the trade association for the commercial pornographers who are the statute's target, use of such verification procedures is "standard practice" in their online operations.

In addition to the monetary cost, and despite strict requirements that identifying information be kept confidential, the identification requirements inherent in age screening may lead some users to fear embarrassment. Both monetary costs and potential embarrassment can deter potential viewers and, in that sense, the statute's requirements may restrict access to a site. But this Court has held that in the context of congressional efforts to protect children, restrictions of this kind do not automatically violate the Constitution. And the Court has approved their use.

In sum, the Act at most imposes a modest additional burden on adult access to legally obscene material, perhaps imposing a similar burden on access to some protected borderline obscene material as well.

II

I turn next to the question of "compelling interest," that of protecting minors from exposure to commercial pornography. No one denies that such an interest is "compelling." Rather, the question here is whether the Act, given its restrictions on adult access, significantly advances that interest. In other words, is the game worth the candle?

The majority argues that it is not, because of the existence of "blocking and filtering software." The majority refers to the presence of that software as a "less restrictive alternative." But that is a misnomer—a misnomer that may lead the reader to believe that all we need do is look to see if the blocking and filtering software is less restrictive; and to believe that, because in one sense it is (one can turn off the software), that is the end of the constitutional matter.

But such reasoning has no place here. Conceptually speaking, the presence of filtering software is not an *alternative* legislative approach to the problem of protecting children from exposure to commercial pornography. Rather, it is part of the status quo, i.e., the backdrop against which Congress enacted the present statute. It is always true, by definition, that the status quo is less restrictive than a new regulatory law. It is always less restrictive to do *nothing* than to do *something*. But "doing nothing" does not address the problem Congress sought to address—namely, that, despite the availability of filtering software, children were still being exposed to harmful material on the Internet.

Thus, the relevant constitutional question is not the question the Court asks: Would it be less restrictive to do nothing? Of course it would be. Rather, the relevant question posits a comparison of (a) a status quo that includes filtering software with (b) a change in that status quo that adds to it an age-verification screen requirement. Given the existence of filtering software, does the problem Congress identified remain significant? Does the Act help to address it? These are questions about the relation of the Act to the compelling interest. Does the Act, compared to the status quo, significantly advance the ball? (An affirmative answer to these questions will not justify "[a]ny restriction on speech," as the Court claims, for a final answer in respect to constitutionality must take account of burdens and alternatives as well.)

The answers to these intermediate questions are clear: Filtering software, as presently available, does not solve the "child protection" problem. It suffers from four serious inadequacies that prompted Congress to pass legislation instead of relying on its voluntary use. First, its filtering is faulty, allowing some pornographic material to pass through without hindrance. Just last year, in American Library Assn., Justice STEVENS described "fundamental defects in the filtering software that is now available or that will be available in the foreseeable future." He pointed to the problem of underblocking: "Because the software relies on key words or phrases to block undesirable sites, it does not have the capacity to exclude a precisely defined category of images." That is to say, in the absence of words, the software alone cannot distinguish between the most obscene pictorial image and the Venus de Milo. No Member of this Court disagreed.

Second, filtering software costs money. Not every family has the $40 or so necessary to install it. By way of contrast, age screening costs less. See supra, at 2800 (citing costs of up to 20 cents per password or $20 per user for an identification number).

Third, filtering software depends upon parents willing to decide where their children will surf the Web and able to enforce that decision. As to millions of American families, that is not a reasonable possibility. More than 28 million school age children have both parents or their sole parent in the work force, at least 5 million children are left alone at home without supervision each week, and many of those children will spend afternoons and evenings with friends who may well have access to computers and more lenient parents.

Fourth, software blocking lacks precision, with the result that those who wish to use it to screen out pornography find that it blocks a great deal of material that is valuable. As Justice STEVENS pointed out, "the software's reliance on words to identify undesirable sites necessarily results in the blocking of thousands of pages that contain content that is completely innocuous for both adults and minors, and that no rational person could conclude matches the filtering companies' category definitions, such as pornography or sex." Indeed, the American Civil Liberties Union (ACLU), one of the respondents here, told Congress that filtering software "block[s] out valuable and protected information, such as information about the Quaker religion, and web sites including those of the American Association of University Women, the AIDS Quilt, the Town Hall Political Site (run by the Family Resource Center, Christian Coalition and other conservative groups)." The software "is simply incapable of discerning between constitutionally protected and unprotected speech." It "inappropriately blocks valuable, protected speech, and does not effectively block the sites [it is] intended to block."

Nothing in the District Court record suggests the contrary. No respondent has offered to produce evidence at trial to the contrary. No party has suggested, for example, that technology allowing filters to interpret and discern among images has suddenly become, or is about to become, widely available. Indeed, the Court concedes that "[f]iltering software, of course, is not a perfect solution to the problem."

In sum, a "filtering software status quo" means filtering that underblocks, imposes a cost upon each family that uses it, fails to screen outside the home, and lacks precision. Thus, Congress could reasonably conclude that a system that relies entirely upon the use of such software is not an effective system. And a law that adds to that system an age-verification screen requirement significantly increases the system's efficacy. That is to say, at a modest additional cost to those adults who wish to obtain access to a screened program, that law will bring about better, more precise blocking, both inside and outside the home.

The Court's response—that 40% of all pornographic material may be of foreign origin—is beside the point. Even assuming (I believe unrealistically) that *all* foreign originators will refuse to use screening, the Act would make a difference in respect to 60% of the Internet's commercial pornography. I cannot call that difference insignificant.

The upshot is that Congress could reasonably conclude that, despite the current availability of filtering software, a child protection problem exists. It also could conclude that a precisely targeted regulatory statute, adding an age-verification requirement for a narrow range of material, would more effectively shield children from commercial pornography.

Is this justification sufficient? The lower courts thought not. But that is because those courts interpreted the Act as imposing far more than a modest burden. They assumed an interpretation of the statute in which it reached far beyond legally obscene and borderline obscene material, affecting material that, given the interpretation set forth above, would fall well outside the Act's scope. But we must interpret the Act to save it, not to destroy it. So interpreted, the Act imposes a far lesser burden on access to protected material. Given the modest nature of that burden and the likelihood that the Act will significantly further Congress' compelling objective, the Act may well satisfy the First Amendment's stringent tests. Indeed, it does satisfy the First Amendment unless, of course, there is a genuine alternative, "less restrictive" way similarly to further that objective.

III

I turn, then, to the actual "less restrictive alternatives" that the Court proposes. The Court proposes two real alternatives, i.e., two potentially less restrictive ways in which Congress might alter the status quo in order to achieve its "compelling" objective.

First, the Government might "act to encourage" the use of blocking and filtering software. The problem is that any argument that rests upon this alternative proves too much. If one imagines enough Government resources devoted to the problem and perhaps additional scientific advances, then, of course, the use of software might become as effective and less restrictive. Obviously, the Government could give all parents, schools, and Internet cafes free computers with filtering programs already installed, hire federal employees to train parents and teachers on their use, and devote millions of dollars to the development of better software. The result might be an alternative that is extremely effective.

But the Constitution does not, because it cannot, require the Government to disprove the existence of magic solutions, i.e., solutions that, put in general terms, will solve any problem less restrictively but with equal effectiveness. Otherwise, "the undoubted ability of lawyers and judges," who are not constrained by the budgetary worries and other practical parameters within which Congress must operate, "to imagine some kind of slightly less drastic or restrictive an approach would make it impossible to write laws that deal with the harm that called the statute into being." As Justice Blackmun recognized, a "judge would be unimaginative indeed if he could not come up with something a little less 'drastic' or a little less 'restrictive' in almost any situation, and thereby enable himself to vote to strike legislation down." Perhaps that is why no party has argued seriously that additional expenditure of government funds to encourage the use of screening is a "less restrictive alternative."

Second, the majority suggests decriminalizing the statute, noting the "chilling effect" of criminalizing a category of speech. To remove a major sanction, however, would make the statute less effective, virtually by definition.

IV

My conclusion is that the Act, as properly interpreted, risks imposition of minor burdens on some protected material—burdens that adults wishing to view the material may overcome at

modest cost. At the same time, it significantly helps to achieve a compelling congressional goal, protecting children from exposure to commercial pornography. There is no serious, practically available "less restrictive" way similarly to further this compelling interest. Hence the Act is constitutional.

V

The Court's holding raises two more general questions. First, what has happened to the "constructive discourse between our courts and our legislatures" that "is an integral and admirable part of the constitutional design"? After eight years of legislative effort, two statutes, and three Supreme Court cases the Court sends this case back to the District Court for further proceedings. What proceedings? I have found no offer by either party to present more relevant evidence. What remains to be litigated? I know the Court says that the parties may "introduce further evidence" as to the "relative restrictiveness and effectiveness of alternatives to the statute." But I do not understand what that new evidence might consist of.

Moreover, Congress passed the current statute "[i]n response to the Court's decision in *Reno* " striking down an earlier statutory effort to deal with the same problem. Congress read *Reno* with care. It dedicated itself to the task of drafting a statute that would meet each and every criticism of the predecessor statute that this Court set forth in *Reno*. It incorporated language from the Court's precedents, particularly the *Miller* standard, virtually verbatim. And it created what it believed was a statute that would protect children from exposure to obscene professional pornography without obstructing adult access to material that the First Amendment protects. See H.R. Rep., at 5 (explaining that the bill was "carefully drafted to respond to the Supreme Court's decision in *Reno*"); S. Rep., at 2 (same). What else was Congress supposed to do?

I recognize that some Members of the Court, now or in the past, have taken the view that the First Amendment simply does not permit Congress to legislate in this area. Others believe that the Amendment does not permit Congress to legislate in certain ways, e.g., through the imposition of criminal penalties for obscenity. There are strong constitutional arguments favoring these views. But the Court itself does not adopt those views. Instead, it finds that the Government has not proved the nonexistence of "less restrictive alternatives." That finding, if appropriate here, is universally appropriate. And if universally appropriate, it denies to Congress, in practice, the legislative leeway that the Court's language seems to promise. If this statute does not pass the Court's "less restrictive alternative" test, what does? If nothing does, then the Court should say so clearly.

As I have explained, I believe the First Amendment permits an alternative holding. We could construe the statute narrowly—as I have tried to do—removing nearly all protected material from its scope. By doing so, we could reconcile its language with the First Amendment's demands. We would "save" the statute, "not ... destroy" it. And in the process, we would permit Congress to achieve its basic child-protecting objectives.

Second, will the majority's holding in practice mean greater or lesser protection for expression? I do not find the answer to this question obvious. The Court's decision removes an important weapon from the prosecutorial arsenal. That weapon would have given the Government a

choice—a choice other than "ban totally or do nothing at all." The Act tells the Government that, instead of prosecuting bans on obscenity to the maximum extent possible (as respondents have urged as yet another "alternative"), it can insist that those who make available material that is obscene or close to obscene keep that material under wraps, making it readily available to adults who wish to see it, while restricting access to children. By providing this third option—a "middle way"—the Act avoids the need for potentially speech-suppressing prosecutions.

That matters in a world where the obscene and the nonobscene do not come tied neatly into separate, easily distinguishable, packages. In that real world, this middle way might well have furthered First Amendment interests by tempering the prosecutorial instinct in borderline cases. At least, Congress might have so believed. And this likelihood, from a First Amendment perspective, might ultimately have proved more protective of the rights of viewers to retain access to expression than the all-or-nothing choice available to prosecutors in the wake of the majority's opinion.

For these reasons, I dissent.

47 U.S.C. § 230. Protection for private blocking and screening of offensive material.

(a) Findings

The Congress finds the following:

(1) The rapidly developing array of Internet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of educational and informational resources to our citizens.

(2) These services offer users a great degree of control over the information that they receive, as well as the potential for even greater control in the future as technology develops.

(3) The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.

(4) The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation.

(5) Increasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services.

(b) Policy

It is the policy of the United States—

(1) to promote the continued development of the Internet and other interactive computer services and other interactive media;

(2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;

(3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;

(4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material; and

(5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

(c) Protection for "Good Samaritan" blocking and screening of offensive material

(1) Treatment of publisher or speaker

No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

(2) Civil liability

No provider or user of an interactive computer service shall be held liable on account of—

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or

otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (A).

(d) Obligations of interactive computer service

A provider of interactive computer service shall, at the time of entering an agreement with a customer for the provision of interactive computer service and in a manner deemed appropriate by the provider, notify such customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors. Such notice shall identify, or provide the customer with access to information identifying, current providers of such protections.

(e) Effect on other laws

(1) No effect on criminal law

Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, or any other Federal criminal statute.

(2) No effect on intellectual property law

Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.

(3) State law

Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.

(4) No effect on communications privacy law

Nothing in this section shall be construed to limit the application of the Electronic Communications Privacy Act of 1986 or any of the amendments made by such Act, or any similar State law.

(f) Definitions

As used in this section:

(1) Internet

The term “Internet” means the international computer network of both Federal and non-Federal interoperable packet switched data networks.

(2) Interactive computer service

The term “interactive computer service” means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

(3) Information content provider

The term “information content provider” means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.

(4) Access software provider

The term “access software provider” means a provider of software (including client or server software), or enabling tools that do any one or more of the following:

(A) filter, screen, allow, or disallow content;

(B) pick, choose, analyze, or digest content; or

(C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.

Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997).
Wilkinson, Chief Judge.

Kenneth Zeran brought this action against America Online, Inc. ("AOL"), arguing that AOL unreasonably delayed in removing defamatory messages posted by an unidentified third party, refused to post retractions of those messages, and failed to screen for similar postings thereafter. The district court granted judgment for AOL on the grounds that the Communications Decency Act of 1996 ("CDA")—47 U.S.C. § 230—bars Zeran's claims. Zeran appeals, arguing that § 230 leaves intact liability for interactive computer service providers who possess notice of defamatory material posted through their services. He also contends that § 230 does not apply here because his claims arise from AOL's alleged negligence prior to the CDA's enactment. Section 230, however, plainly immunizes computer service providers like AOL from liability for information that originates with third parties. Furthermore, Congress clearly expressed its intent that § 230 apply to lawsuits, like Zeran's, instituted after the CDA's enactment. Accordingly, we affirm the judgment of the district court.

I.

"The Internet is an international network of interconnected computers," currently used by approximately 40 million people worldwide. One of the many means by which individuals access the Internet is through an interactive computer service. These services offer not only a connection to the Internet as a whole, but also allow their subscribers to access information communicated and stored only on each computer service's individual proprietary network. AOL is just such an interactive computer service. Much of the information transmitted over its network originates with the company's millions of subscribers. They may transmit information privately via electronic mail, or they may communicate publicly by posting messages on AOL bulletin boards, where the messages may be read by any AOL subscriber.

The instant case comes before us on a motion for judgment on the pleadings, so we accept the facts alleged in the complaint as true. On April 25, 1995, an unidentified person posted a message on an AOL bulletin board advertising "Naughty Oklahoma T-Shirts." The posting described the sale of shirts featuring offensive and tasteless slogans related to the April 19, 1995, bombing of the Alfred P. Murrah Federal Building in Oklahoma City. Those interested in purchasing the shirts were instructed to call "Ken" at Zeran's home phone number in Seattle, Washington. As a result of this anonymously perpetrated prank, Zeran received a high volume of calls, comprised primarily of angry and derogatory messages, but also including death threats. Zeran could not change his phone number because he relied on its availability to the public in running his business out of his home. Later that day, Zeran called AOL and informed a company representative of his predicament. The employee assured Zeran that the posting would be removed from AOL's bulletin board but explained that as a matter of policy AOL would not post a retraction. The parties dispute the date that AOL removed this original posting from its bulletin board.

On April 26, the next day, an unknown person posted another message advertising additional shirts with new tasteless slogans related to the Oklahoma City bombing. Again, interested buyers were told to call Zeran's phone number, to ask for "Ken," and to "please call back if busy" due

to high demand. The angry, threatening phone calls intensified. Over the next four days, an unidentified party continued to post messages on AOL's bulletin board, advertising additional items including bumper stickers and key chains with still more offensive slogans. During this time period, Zeran called AOL repeatedly and was told by company representatives that the individual account from which the messages were posted would soon be closed. Zeran also reported his case to Seattle FBI agents. By April 30, Zeran was receiving an abusive phone call approximately every two minutes.

Meanwhile, an announcer for Oklahoma City radio station KRXO received a copy of the first AOL posting. On May 1, the announcer related the message's contents on the air, attributed them to "Ken" at Zeran's phone number, and urged the listening audience to call the number. After this radio broadcast, Zeran was inundated with death threats and other violent calls from Oklahoma City residents. Over the next few days, Zeran talked to both KRXO and AOL representatives. He also spoke to his local police, who subsequently surveilled his home to protect his safety. By May 14, after an Oklahoma City newspaper published a story exposing the shirt advertisements as a hoax and after KRXO made an on-air apology, the number of calls to Zeran's residence finally subsided to fifteen per day.

Zeran first filed suit on January 4, 1996, against radio station KRXO in the United States District Court for the Western District of Oklahoma. On April 23, 1996, he filed this separate suit against AOL in the same court. Zeran did not bring any action against the party who posted the offensive messages.[1] After Zeran's suit against AOL was transferred to the Eastern District of Virginia pursuant to 28 U.S.C. § 1404(a), AOL answered Zeran's complaint and interposed 47 U.S.C. § 230 as an affirmative defense. AOL then moved for judgment on the pleadings pursuant to Fed.R.Civ.P. 12(c). The district court granted AOL's motion, and Zeran filed this appeal.

II.

A.

Because § 230 was successfully advanced by AOL in the district court as a defense to Zeran's claims, we shall briefly examine its operation here. Zeran seeks to hold AOL liable for defamatory speech initiated by a third party. He argued to the district court that once he notified AOL of the unidentified third party's hoax, AOL had a duty to remove the defamatory posting promptly, to notify its subscribers of the message's false nature, and to effectively screen future defamatory material. Section 230 entered this litigation as an affirmative defense pled by AOL. The company claimed that Congress immunized interactive computer service providers from claims based on information posted by a third party.

The relevant portion of § 230 states: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[2] By its plain language, § 230 creates a federal immunity to any cause of action

[1] Zeran maintains that AOL made it impossible to identify the original party by failing to maintain adequate records of its users. The issue of AOL's record keeping practices, however, is not presented by this appeal.

[2] …The parties do not dispute that AOL falls within the CDA's "interactive computer service" definition and that the unidentified third party who posted the offensive messages here fits the definition of an "information content provider."

that would make service providers liable for information originating with a third-party user of the service. Specifically, § 230 precludes courts from entertaining claims that would place a computer service provider in a publisher's role. Thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content-are barred.

The purpose of this statutory immunity is not difficult to discern. Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium. The imposition of tort liability on service providers for the communications of others represented, for Congress, simply another form of intrusive government regulation of speech. Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum. In specific statutory findings, Congress recognized the Internet and interactive computer services as offering "a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity." It also found that the Internet and interactive computer services "have flourished, to the benefit of all Americans, *with a minimum of government regulation*." (emphasis added). Congress further stated that it is "the policy of the United States ... to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, *unfettered by Federal or State regulation*." (emphasis added).

None of this means, of course, that the original culpable party who posts defamatory messages would escape accountability. While Congress acted to keep government regulation of the Internet to a minimum, it also found it to be the policy of the United States "to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer." Congress made a policy choice, however, not to deter harmful online speech through the separate route of imposing tort liability on companies that serve as intermediaries for other parties' potentially injurious messages.

Congress' purpose in providing the § 230 immunity was thus evident. Interactive computer services have millions of users. The amount of information communicated via interactive computer services is therefore staggering. The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It would be impossible for service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted. Congress considered the weight of the speech interests implicated and chose to immunize service providers to avoid any such restrictive effect.

Another important purpose of § 230 was to encourage service providers to self-regulate the dissemination of offensive material over their services. In this respect, § 230 responded to a New York state court decision, Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 (N.Y.Sup.Ct. May 24, 1995). There, the plaintiffs sued Prodigy—an interactive computer service like AOL—for defamatory comments made by an unidentified party on one of Prodigy's bulletin boards. The court held Prodigy to the strict liability standard normally applied to original publishers of defamatory statements, rejecting Prodigy's claims that it should be held only to the

lower “knowledge” standard usually reserved for distributors. The court reasoned that Prodigy acted more like an original publisher than a distributor both because it advertised its practice of controlling content on its service and because it actively screened and edited messages posted on its bulletin boards.

Congress enacted § 230 to remove the disincentives to self-regulation created by the *Stratton Oakmont* decision. Under that court’s holding, computer service providers who regulated the dissemination of offensive material on their services risked subjecting themselves to liability, because such regulation cast the service provider in the role of a publisher. Fearing that the specter of liability would therefore deter service providers from blocking and screening offensive material, Congress enacted § 230’s broad immunity “to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children’s access to objectionable or inappropriate online material.” In line with this purpose, § 230 forbids the imposition of publisher liability on a service provider for the exercise of its editorial and self-regulatory functions.

B.

Zeran argues, however, that the § 230 immunity eliminates only publisher liability, leaving distributor liability intact. Publishers can be held liable for defamatory statements contained in their works even absent proof that they had specific knowledge of the statement’s inclusion. W. Page Keeton et al., Prosser and Keeton on the Law of Torts § 113, at 810 (5th ed. 1984). According to Zeran, interactive computer service providers like AOL are normally considered instead to be distributors, like traditional news vendors or book sellers. Distributors cannot be held liable for defamatory statements contained in the materials they distribute unless it is proven at a minimum that they have actual knowledge of the defamatory statements upon which liability is predicated. Id. at 811 (explaining that distributors are not liable “in the absence of proof that they knew or had reason to know of the existence of defamatory matter contained in matter published”). Zeran contends that he provided AOL with sufficient notice of the defamatory statements appearing on the company’s bulletin board. This notice is significant, says Zeran, because AOL could be held liable as a distributor only if it acquired knowledge of the defamatory statements’ existence.

Because of the difference between these two forms of liability, Zeran contends that the term “distributor” carries a legally distinct meaning from the term “publisher.” Accordingly, he asserts that Congress’ use of only the term “publisher” in § 230 indicates a purpose to immunize service providers only from publisher liability. He argues that distributors are left unprotected by § 230 and, therefore, his suit should be permitted to proceed against AOL. We disagree. Assuming *arguendo* that Zeran has satisfied the requirements for imposition of distributor liability, this theory of liability is merely a subset, or a species, of publisher liability, and is therefore also foreclosed by § 230.

The terms “publisher” and “distributor” derive their legal significance from the context of defamation law. Although Zeran attempts to artfully plead his claims as ones of negligence, they are indistinguishable from a garden variety defamation action. Because the publication of a statement is a necessary element in a defamation action, only one who publishes can be subject

to this form of tort liability. Restatement (Second) of Torts § 558(b) (1977); Keeton et al., supra, § 113, at 802. Publication does not only describe the choice by an author to include certain information. In addition, both the negligent communication of a defamatory statement and the failure to remove such a statement when first communicated by another party—each alleged by Zeran here under a negligence label—constitute publication. Restatement (Second) of Torts § 577. In fact, every repetition of a defamatory statement is considered a publication. Keeton et al., supra, § 113, at 799.

In this case, AOL is legally considered to be a publisher. "[E]very one who takes part in the publication ... is charged with publication." Id. Even distributors are considered to be publishers for purposes of defamation law:

> Those who are in the business of making their facilities available to disseminate the writings composed, the speeches made, and the information gathered by others may also be regarded as participating to such an extent in making the books, newspapers, magazines, and information available to others as to be regarded as publishers. They are intentionally making the contents available to others, sometimes without knowing all of the contents-including the defamatory content-and sometimes without any opportunity to ascertain, in advance, that any defamatory matter was to be included in the matter published.

Id. at 803. AOL falls squarely within this traditional definition of a publisher and, therefore, is clearly protected by § 230's immunity.

Zeran contends that decisions like *Stratton Oakmont* and Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y. 1991), recognize a legal distinction between publishers and distributors. He misapprehends, however, the significance of that distinction for the legal issue we consider here. It is undoubtedly true that mere conduits, or distributors, are subject to a different standard of liability. As explained above, distributors must at a minimum have knowledge of the existence of a defamatory statement as a prerequisite to liability. But this distinction signifies only that different standards of liability may be applied *within* the larger publisher category, depending on the specific type of publisher concerned. See Keeton et al., supra, § 113, at 799-800 (explaining that every party involved is charged with publication, although degrees of legal responsibility differ). To the extent that decisions like *Stratton* and *Cubby* utilize the terms "publisher" and "distributor" separately, the decisions correctly describe two different standards of liability. *Stratton* and *Cubby* do not, however, suggest that distributors are not also a type of publisher for purposes of defamation law.

Zeran simply attaches too much importance to the presence of the distinct notice element in distributor liability. The simple fact of notice surely cannot transform one from an original publisher to a distributor in the eyes of the law. To the contrary, once a computer service provider receives notice of a potentially defamatory posting, it is thrust into the role of a traditional publisher. The computer service provider must decide whether to publish, edit, or withdraw the posting. In this respect, Zeran seeks to impose liability on AOL for assuming the role for which § 230 specifically proscribes liability—the publisher role.

Our view that Zeran's complaint treats AOL as a publisher is reinforced because AOL is cast in the same position as the party who originally posted the offensive messages. According to Zeran's logic, AOL is legally at fault because it communicated to third parties an allegedly defamatory statement. This is precisely the theory under which the original poster of the offensive messages would be found liable. If the original party is considered a publisher of the offensive messages, Zeran certainly cannot attach liability to AOL under the same theory without conceding that AOL too must be treated as a publisher of the statements.

Zeran next contends that interpreting § 230 to impose liability on service providers with knowledge of defamatory content on their services is consistent with the statutory purposes outlined in Part IIA. Zeran fails, however, to understand the practical implications of notice liability in the interactive computer service context. Liability upon notice would defeat the dual purposes advanced by § 230 of the CDA. Like the strict liability imposed by the *Stratton Oakmont* court, liability upon notice reinforces service providers' incentives to restrict speech and abstain from self-regulation.

If computer service providers were subject to distributor liability, they would face potential liability each time they receive notice of a potentially defamatory statement—from any party, concerning any message. Each notification would require a careful yet rapid investigation of the circumstances surrounding the posted information, a legal judgment concerning the information's defamatory character, and an on-the-spot editorial decision whether to risk liability by allowing the continued publication of that information. Although this might be feasible for the traditional print publisher, the sheer number of postings on interactive computer services would create an impossible burden in the Internet context. Cf. Auvil v. CBS 60 Minutes, 800 F. Supp. 928, 931 (E.D. Wash. 1992) (recognizing that it is unrealistic for network affiliates to "monitor incoming transmissions and exercise on-the-spot discretionary calls"). Because service providers would be subject to liability only for the publication of information, and not for its removal, they would have a natural incentive simply to remove messages upon notification, whether the contents were defamatory or not. Thus, like strict liability, liability upon notice has a chilling effect on the freedom of Internet speech.

Similarly, notice-based liability would deter service providers from regulating the dissemination of offensive material over their own services. Any efforts by a service provider to investigate and screen material posted on its service would only lead to notice of potentially defamatory material more frequently and thereby create a stronger basis for liability. Instead of subjecting themselves to further possible lawsuits, service providers would likely eschew any attempts at self-regulation.

More generally, notice-based liability for interactive computer service providers would provide third parties with a no-cost means to create the basis for future lawsuits. Whenever one was displeased with the speech of another party conducted over an interactive computer service, the offended party could simply "notify" the relevant service provider, claiming the information to be legally defamatory. In light of the vast amount of speech communicated through interactive computer services, these notices could produce an impossible burden for service providers, who would be faced with ceaseless choices of suppressing controversial speech or sustaining prohibitive liability. Because the probable effects of distributor liability on the vigor of Internet

speech and on service provider self-regulation are directly contrary to § 230's statutory purposes, we will not assume that Congress intended to leave liability upon notice intact….

Fair Housing Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008) (en banc)
Kozinski, Chief Judge.

We plumb the depths of the immunity provided by section 230 of the Communications Decency Act of 1996 ("CDA").

Facts[1]

Defendant Roommate.com, LLC ("Roommate") operates a website designed to match people renting out spare rooms with people looking for a place to live.[2] At the time of the district court's disposition, Roommate's website featured approximately 150,000 active listings and received around a million page views a day. Roommate seeks to profit by collecting revenue from advertisers and subscribers.

Before subscribers can search listings or post housing opportunities on Roommate's website, they must create profiles, a process that requires them to answer a series of questions. In addition to requesting basic information—such as name, location and email address—Roommate requires each subscriber to disclose his sex, sexual orientation and whether he would bring children to a household. Each subscriber must also describe his preferences in roommates with respect to the same three criteria: sex, sexual orientation and whether they will bring children to the household. The site also encourages subscribers to provide "Additional Comments" describing themselves and their desired roommate in an open-ended essay. After a new subscriber completes the application, Roommate assembles his answers into a "profile page." The profile page displays the subscriber's pseudonym, his description and his preferences, as divulged through answers to Roommate's questions.

Subscribers can choose between two levels of service: Those using the site's free service level can create their own personal profile page, search the profiles of others and send personal email messages. They can also receive periodic emails from Roommate, informing them of available housing opportunities matching their preferences. Subscribers who pay a monthly fee also gain the ability to read emails from other users, and to view other subscribers' "Additional Comments."

The Fair Housing Councils of the San Fernando Valley and San Diego ("Councils") sued Roommate in federal court, alleging that Roommate's business violates the federal Fair Housing Act ("FHA") and California housing discrimination laws. Councils claim that Roommate is effectively a housing broker doing online what it may not lawfully do off-line. The district court held that Roommate is immune under section 230 of the CDA and dismissed the federal claims without considering whether Roommate's actions violated the FHA. The court then declined to exercise supplemental jurisdiction over the state law claims. Councils appeal the dismissal of the FHA claim and Roommate cross-appeals the denial of attorneys' fees.

[1] This appeal is taken from the district court's order granting defendant's motion for summary judgment, so we view contested facts in the light most favorable to plaintiffs.
[2] For unknown reasons, the company goes by the singular name "Roommate.com, LLC" but pluralizes its website's URL, www.roommates.com.

Analysis

Section 230 of the CDA immunizes providers of interactive computer services[6] against liability arising from content created by third parties: "No provider ... of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." This grant of immunity applies only if the interactive computer service provider is not also an "information content provider," which is defined as someone who is "responsible, in whole or in part, for the creation or development of" the offending content.

A website operator can be both a service provider and a content provider: If it passively displays content that is created entirely by third parties, then it is only a service provider with respect to that content. But as to content that it creates itself, or is "responsible, in whole or in part" for creating or developing, the website is also a content provider. Thus, a website may be immune from liability for some of the content it displays to the public but be subject to liability for other content.

Section 230 was prompted by a state court case holding Prodigy responsible for a libelous message posted on one of its financial message boards. See Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995) (unpublished). The court there found that Prodigy had become a "publisher" under state law because it voluntarily deleted some messages from its message boards "on the basis of offensiveness and 'bad taste,'" and was therefore legally responsible for the content of defamatory messages that it failed to delete. The *Stratton Oakmont* court reasoned that Prodigy's decision to perform some voluntary self-policing made it akin to a newspaper publisher, and thus responsible for messages on its bulletin board that defamed third parties. The court distinguished Prodigy from CompuServe, which had been released from liability in a similar defamation case because CompuServe "had no opportunity to review the contents of the publication at issue before it was uploaded into CompuServe's computer banks." Id.; see Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 140 (S.D.N.Y. 1991). Under the reasoning of *Stratton Oakmont*, online service providers that voluntarily filter some messages become liable for all messages transmitted, whereas providers that bury their heads in the sand and ignore problematic posts altogether escape liability. Prodigy claimed that the "sheer volume" of message board postings it received—at the time, over 60,000 a day—made manual review of every message impossible; thus, if it were forced to choose between taking responsibility for all messages and deleting no messages at all, it would have to choose the latter course.

In passing section 230, Congress sought to spare interactive computer services this grim choice by allowing them to perform some editing on user-generated content without thereby becoming liable for all defamatory or otherwise unlawful messages that they didn't edit or delete. In other words, Congress sought to immunize the removal of user-generated content, not the creation of content: "[S]ection [230] provides 'Good Samaritan' protections from civil liability for providers ... of an interactive computer service for actions to *restrict* ... access to objectionable online material. One of the specific purposes of this section is to overrule *Stratton-Oakmont* [sic] v.

[6] … Today, the most common interactive computer services are websites. Councils do not dispute that Roommate's website is an interactive computer service.

Prodigy and any other similar decisions which have treated such providers ... as publishers or speakers of content that is not their own *because they have restricted access to objectionable material*." H.R.Rep. No. 104-458 (1996) (emphasis added). Indeed, the section is titled "Protection for 'good samaritan' blocking and screening of offensive material" and, as the Seventh Circuit recently held, the substance of section 230(c) can and should be interpreted consistent with its caption. Chicago Lawyers' Committee for Civil Rights Under Law, Inc. v. craigslist, Inc., 519 F.3d 666 (7th Cir. 2008).

With this backdrop in mind, we examine three specific functions performed by Roommate that are alleged to violate the Fair Housing Act and California law.

1. Councils first argue that the questions Roommate poses to prospective subscribers during the registration process violate the Fair Housing Act and the analogous California law. Councils allege that requiring subscribers to disclose their sex, family status and sexual orientation "indicates" an intent to discriminate against them, and thus runs afoul of both the FHA and state law.[13]

Roommate created the questions and choice of answers, and designed its website registration process around them. Therefore, Roommate is undoubtedly the "information content provider" as to the questions and can claim no immunity for posting them on its website, or for forcing subscribers to answer them as a condition of using its services.

Here, we must determine whether Roommate has immunity under the CDA because Councils have at least a plausible claim that Roommate violated state and federal law by merely posing the questions. We need not decide whether any of Roommate's questions actually violate the Fair Housing Act or California law, or whether they are protected by the First Amendment or other constitutional guarantees; we leave those issues for the district court on remand. Rather, we examine the scope of plaintiffs' substantive claims only insofar as necessary to determine whether section 230 immunity applies. However, we note that asking questions certainly *can* violate the Fair Housing Act and analogous laws in the physical world. For example, a real estate broker may not inquire as to the race of a prospective buyer, and an employer may not inquire as to the religion of a prospective employee. If such questions are unlawful when posed face-to-face or by telephone, they don't magically become lawful when asked electronically online. The Communications Decency Act was not meant to create a lawless no-man's-land on the Internet.[15]

---

[13] The Fair Housing Act prohibits any "statement ... with respect to the sale or rental of a dwelling that *indicates ... an intention* to make [a] preference, limitation, or discrimination" on the basis of a protected category. 42 U.S.C. § 3604(c) (emphasis added). California law prohibits "any written or oral inquiry concerning the" protected status of a housing seeker. Cal. Gov.Code § 12955(b).

[15] The dissent stresses the importance of the Internet to modern life and commerce, and we, of course, agree: The Internet is no longer a fragile new means of communication that could easily be smothered in the cradle by overzealous enforcement of laws and regulations applicable to brick-and-mortar businesses. Rather, it has become a dominant—perhaps the preeminent—means through which commerce is conducted. And its vast reach into the lives of millions is exactly why we must be careful not to exceed the scope of the immunity provided by Congress and thus give online businesses an unfair advantage over their real-world counterparts, which must comply with laws of general applicability.

Councils also claim that requiring subscribers to answer the questions as a condition of using Roommate's services unlawfully "cause[s]" subscribers to make a "statement ... with respect to the sale or rental of a dwelling that indicates [a] preference, limitation, or discrimination," in violation of 42 U.S.C. § 3604(c). The CDA does not grant immunity for inducing third parties to express illegal preferences. Roommate's own acts—posting the questionnaire and requiring answers to it—are entirely its doing and thus section 230 of the CDA does not apply to them. Roommate is entitled to no immunity.

2. Councils also charge that Roommate's development and display of subscribers' discriminatory preferences is unlawful. Roommate publishes a "profile page" for each subscriber on its website. The page describes the client's personal information—such as his sex, sexual orientation and whether he has children—as well as the attributes of the housing situation he seeks. The content of these pages is drawn directly from the registration process: For example, Roommate requires subscribers to specify, using a drop-down menu provided by Roommate, whether they are "Male" or "Female" and then displays that information on the profile page. Roommate also requires subscribers who are listing available housing to disclose whether there are currently "Straight male(s)," "Gay male(s)," "Straight female(s)" or "Lesbian(s)" living in the dwelling. Subscribers who are seeking housing must make a selection from a drop-down menu, again provided by Roommate, to indicate whether they are willing to live with "Straight or gay" males, only with "Straight" males, only with "Gay" males or with "No males." Similarly, Roommate requires subscribers listing housing to disclose whether there are "Children present" or "Children not present" and requires housing seekers to say "I will live with children" or "I will not live with children." Roommate then displays these answers, along with other information, on the subscriber's profile page. This information is obviously included to help subscribers decide which housing opportunities to pursue and which to bypass. In addition, Roommate itself uses this information to channel subscribers away from listings where the individual offering housing has expressed preferences that aren't compatible with the subscriber's answers.

The dissent tilts at windmills when it shows, quite convincingly, that Roommate's *subscribers* are information content providers who create the profiles by picking among options and providing their own answers. There is no disagreement on this point. But, the fact that users are information content providers does not preclude Roommate from *also* being an information content provider by helping "develop" at least "in part" the information in the profiles. As we explained in *Batzel*, the party responsible for putting information online may be subject to liability, even if the information originated with a user. See Batzel v. Smith, 333 F.3d 1018, 1033 (9th Cir. 2003).

Here, the part of the profile that is alleged to offend the Fair Housing Act and state housing discrimination laws—the information about sex, family status and sexual orientation—is provided by subscribers in response to Roommate's questions, which they cannot refuse to answer if they want to use defendant's services. By requiring subscribers to provide the information as a condition of accessing its service, and by providing a limited set of pre-populated answers, Roommate becomes much more than a passive transmitter of information provided by others; it becomes the developer, at least in part, of that information. And section 230 provides immunity only if the interactive computer service does not "creat[e] or develop[ ]" the information "in whole or in part."

Our dissenting colleague takes a much narrower view of what it means to "develop" information online, and concludes that Roommate does not develop the information because "[a]ll Roommate does is to provide a form with options for standardized answers." But Roommate does much more than provide options. To begin with, it asks discriminatory questions that even the dissent grudgingly admits are not entitled to CDA immunity. The FHA makes it unlawful to ask certain discriminatory questions for a very good reason: Unlawful questions solicit (a.k.a. "develop") unlawful answers. Not only does Roommate ask these questions, Roommate makes answering the discriminatory questions a condition of doing business. This is no different from a real estate broker in real life saying, "Tell me whether you're Jewish or you can find yourself another broker." When a business enterprise extracts such information from potential customers as a condition of accepting them as clients, it is no stretch to say that the enterprise is responsible, at least in part, for developing that information. For the dissent to claim that the information in such circumstances is "created solely by" the customer, and that the business has not helped in the least to develop it, strains both credulity and English.[19]

Roommate also argues that it is not responsible for the information on the profile page because it is each subscriber's action that leads to publication of his particular profile—in other words, the user pushes the last button or takes the last act before publication. We are not convinced that this is even true, but don't see why it matters anyway. The projectionist in the theater may push the last button before a film is displayed on the screen, but surely this doesn't make him the sole producer of the movie. By any reasonable use of the English language, Roommate is "responsible" at least "in part" for each subscriber's profile page, because every such page is a collaborative effort between Roommate and the subscriber.

Similarly, Roommate is not entitled to CDA immunity for the operation of its search system, which filters listings, or of its email notification system, which directs emails to subscribers according to discriminatory criteria. Roommate designed its search system so it would steer users based on the preferences and personal characteristics that Roommate itself forces subscribers to disclose. If Roommate has no immunity for asking the discriminatory questions, as we concluded above, it can certainly have no immunity for using the answers to the unlawful questions to limit who has access to housing.

For example, a subscriber who self-identifies as a "Gay male" will not receive email notifications of new housing opportunities supplied by owners who limit the universe of acceptable tenants to "Straight male(s)," "Straight female(s)" and "Lesbian(s)." Similarly, subscribers with children will not be notified of new listings where the owner specifies "no children." Councils charge that limiting the information a subscriber can access based on that subscriber's protected status violates the Fair Housing Act and state housing discrimination laws. It is, Councils allege, no different from a real estate broker saying to a client: "Sorry, sir, but I

[19] The dissent may be laboring under a misapprehension as to how the Roommate website is alleged to operate. For example, the dissent spends some time explaining that certain portions of the user profile application are voluntary. We do not discuss these because plaintiffs do not base their claims on the voluntary portions of the application, except the "Additional Comments" portion, discussed below. The dissent also soft-pedals Roommate's influence on the mandatory portions of the applications by referring to it with such words as "encourage" or "encouragement" or "solicitation." Roommate, of course, does much more than encourage or solicit; it forces users to answer certain questions and thereby provide information that other clients can use to discriminate unlawfully.

can't show you any listings on this block because you are [gay/female/black/a parent]." If such screening is prohibited when practiced in person or by telephone, we see no reason why Congress would have wanted to make it lawful to profit from it online.

Roommate's search function is similarly designed to steer users based on discriminatory criteria. Roommate's search engine thus differs materially from generic search engines such as Google, Yahoo! and MSN Live Search, in that Roommate designed its system to use allegedly unlawful criteria so as to limit the results of each search, and to force users to participate in its discriminatory process. In other words, Councils allege that Roommate's search is designed to make it more difficult or impossible for individuals with certain protected characteristics to find housing-something the law prohibits. By contrast, ordinary search engines do not use unlawful criteria to limit the scope of searches conducted on them, nor are they designed to achieve illegal ends-as Roommate's search function is alleged to do here. Therefore, such search engines play no part in the "development" of any unlawful searches.

It's true that the broadest sense of the term "develop" could include the functions of an ordinary search engine—indeed, just about any function performed by a website. But to read the term so broadly would defeat the purposes of section 230 by swallowing up every bit of the immunity that the section otherwise provides. At the same time, reading the exception for co-developers as applying only to content that originates entirely with the website—as the dissent would seem to suggest—ignores the words "development ... in part" in the statutory passage "creation *or development* in whole *or in part*." (emphasis added). We believe that both the immunity for passive conduits and the exception for co-developers must be given their proper scope and, to that end, we interpret the term "development" as referring not merely to augmenting the content generally, but to materially contributing to its alleged unlawfulness. In other words, a website helps to develop unlawful content, and thus falls within the exception to section 230, if it contributes materially to the alleged illegality of the conduct.

The dissent accuses us of "rac[ing] past the plain language of the statute," but we clearly do pay close attention to the statutory language, particularly the word "develop," which we spend many pages exploring. The dissent may disagree with our definition of the term, which is entirely fair, but surely our dissenting colleague is mistaken in suggesting we ignore the term. Nor is the statutory language quite as plain as the dissent would have it. Quoting selectively from the dictionary, the dissent comes up with an exceedingly narrow definition of this rather complex and multi faceted term.[22] Dissent at 1184 (defining development as "gradual advance or growth through progressive changes") (quoting *Webster's Third New International Dictionary* 618 (2002)). The dissent does not pause to consider how such a definition could apply to website content at all, as it excludes the kinds of swift and disorderly changes that are the hallmark of growth on the Internet. Had our dissenting colleague looked just a few lines lower on the same page of the same edition of the same dictionary, she would have found another definition of "development" that is far more suitable to the context in which we operate: "making usable or

[22] Development, it will be recalled, has many meanings, which differ materially depending on context. Thus, "development" when used as part of the phrase "research and development" means something quite different than when referring to "mental development," and something else again when referring to "real estate development," "musical development" or "economic development."

available." The dissent does not explain why the definition it has chosen reflects the statute's "plain meaning," while the ones it bypasses do not.

More fundamentally, the dissent does nothing at all to grapple with the difficult statutory problem posed by the fact that section 230(c) uses both "create" and "develop" as separate bases for loss of immunity. Everything that the dissent includes within its cramped definition of "development" fits just as easily within the definition of "creation"—which renders the term "development" superfluous. The dissent makes no attempt to explain or offer examples as to how its interpretation of the statute leaves room for "development" as a separate basis for a website to lose its immunity, yet we are advised by the Supreme Court that we must give meaning to all statutory terms, avoiding redundancy or duplication wherever possible.

While content to pluck the "plain meaning" of the statute from a dictionary definition that predates the Internet by decades, *compare Webster's Third New International Dictionary* 618 (1963) with *Webster's Third New International Dictionary* 618 (2002) (both containing "gradual advance or growth through progressive changes"), the dissent overlooks the far more relevant definition of "[web] content development" in Wikipedia: "the process of researching, writing, gathering, organizing and editing information for publication on web sites." Our interpretation of "development" is entirely in line with the context-appropriate meaning of the term, and easily fits the activities Roommate engages in.

In an abundance of caution, and to avoid the kind of misunderstanding the dissent seems to encourage, we offer a few examples to elucidate what does and does not amount to "development" under section 230 of the Communications Decency Act: If an individual uses an ordinary search engine to query for a "white roommate," the search engine has not contributed to any alleged unlawfulness in the individual's conduct; providing *neutral* tools to carry out what may be unlawful or illicit searches does not amount to "development" for purposes of the immunity exception. A dating website that requires users to enter their sex, race, religion and marital status through drop-down menus, and that provides means for users to search along the same lines, retains its CDA immunity insofar as it does not contribute to any alleged illegality;[23] this immunity is retained even if the website is sued for libel based on these characteristics because the website would not have contributed materially to any alleged defamation. Similarly, a housing website that allows users to specify whether they will or will not receive emails by means of *user-defined* criteria might help some users exclude email from other users of a particular race or sex. However, that website would be immune, so long as it does not require the use of discriminatory criteria. A website operator who edits user-created content—such as by correcting spelling, removing obscenity or trimming for length—retains his immunity for any illegality in the user-created content, provided that the edits are unrelated to the illegality. However, a website operator who edits in a manner that contributes to the alleged illegality—such as by removing the word "not" from a user's message reading "[Name] did *not* steal the artwork" in order to transform an innocent message into a libelous one—is directly involved in the alleged illegality and thus not immune.[24]

[23] It is perfectly legal to discriminate along those lines in dating, and thus there can be no claim based solely on the content of these questions.

[24] Requiring website owners to refrain from taking affirmative acts that are unlawful does not strike us as an undue burden. These are, after all, businesses that are being held responsible only for their own conduct; there is no

Here, Roommate's connection to the discriminatory filtering process is direct and palpable: Roommate designed its search and email systems to limit the listings available to subscribers based on sex, sexual orientation and presence of children.[25] Roommate selected the criteria used to hide listings, and Councils allege that the act of hiding certain listings is itself unlawful under the Fair Housing Act, which prohibits brokers from steering clients in accordance with discriminatory preferences.[26] We need not decide the merits of Councils' claim to hold that Roommate is sufficiently involved with the design and operation of the search and email systems—which are engineered to limit access to housing on the basis of the protected characteristics elicited by the registration process—so as to forfeit any immunity to which it was otherwise entitled under section 230.

Roommate's situation stands in stark contrast to *Stratton Oakmont*, the case Congress sought to reverse through passage of section 230. There, defendant Prodigy was held liable for a user's unsolicited message because it attempted to *remove* some problematic content from its website, but didn't remove enough. Here, Roommate is not being sued for removing some harmful messages while failing to remove others; instead, it is being sued for the predictable consequences of creating a website designed to solicit and enforce housing preferences that are alleged to be illegal.

We take this opportunity to clarify two of our previous rulings regarding the scope of section 230 immunity. Today's holding sheds additional light on Batzel v. Smith, 333 F.3d 1018 (9th Cir. 2003). There, the editor of an email newsletter received a tip about some artwork, which the tipster falsely alleged to be stolen. The newsletter editor incorporated the tipster's email into the next issue of his newsletter and added a short headnote, which he then emailed to his subscribers.[27] The art owner sued for libel and a split panel held the newsletter editor to be immune under section 230 of the CDA.[28]

---

vicarious liability for the misconduct of their customers. Compliance with laws of general applicability seems like an entirely justified burden for all businesses, whether they operate online or through quaint brick-and-mortar facilities. Insofar, however, as a plaintiff would bring a claim under state or federal law based on a website operator's passive acquiescence in the misconduct of its users, the website operator would likely be entitled to CDA immunity. This is true even if the users committed their misconduct using electronic tools of general applicability provided by the website operator.

[25] Of course, the logic of Roommate's argument is not limited to discrimination based on these particular criteria. If Roommate were free to discriminate in providing housing services based on sex, there is no reason another website could not discriminate based on race, religion or national origin. Nor is its logic limited to housing; it would apply equally to websites providing employment or educational opportunities—or anything else, for that matter.

[26] The dissent argues that Roommate is not liable because the decision to discriminate on these grounds does not originate with Roommate; instead, "users have chosen to select characteristics that they find desirable." But, it is Roommate that *forces* users to express a preference and Roommate that forces users to disclose the information that can form the basis of discrimination by others. Thus, Roommate makes discrimination both possible and respectable.

[27] Apparently, it was common practice for this editor to receive and forward tips from his subscribers. In effect, the newsletter served as a heavily moderated discussion list.

[28] As an initial matter, the *Batzel* panel held that the defendant newsletter editor was a "user" of an interactive computer service within the definition provided by section 230. While we have our doubts, we express no view on this issue because it is not presented to us. Thus, we assume that the editor fell within the scope of section 230's coverage without endorsing *Batzel's* analysis on this point.

Our opinion is entirely consistent with that part of *Batzel* which holds that an editor's minor changes to the spelling, grammar and length of third-party content do not strip him of section 230 immunity. None of those changes contributed to the libelousness of the message, so they do not add up to "development" as we interpret the term. *Batzel* went on to hold that the editor *could* be liable for selecting the tipster's email for inclusion in the newsletter, depending on whether or not the tipster had tendered the piece to the editor for posting online, and remanded for a determination of that issue.

The distinction drawn by *Batzel* anticipated the approach we take today. As *Batzel* explained, if the tipster tendered the material for posting online, then the editor's job was, essentially, to determine whether or not to prevent its posting—precisely the kind of activity for which section 230 was meant to provide immunity.[29] And any activity that can be boiled down to deciding whether to exclude material that third parties seek to post online is perforce immune under section 230. But if the editor publishes material that he does not believe was tendered to him for posting online, then he is the one making the affirmative decision to publish, and so he contributes materially to its allegedly unlawful dissemination. He is thus properly deemed a developer and not entitled to CDA immunity.[30]

We must also clarify the reasoning undergirding our holding in Carafano v. Metrosplash.com, Inc., 339 F.3d 1119 (9th Cir. 2003), as we used language there that was unduly broad. In *Carafano*, an unknown prankster impersonating actress Christianne Carafano created a profile for her on an online dating site. The profile included Carafano's home address and suggested that she was looking for an unconventional liaison. When Carafano received threatening phone calls, she sued the dating site for publishing the unauthorized profile. The site asserted immunity under section 230. We correctly held that the website was immune, but incorrectly suggested that it could never be liable because "no [dating] profile has any content until a user actively creates it." As we explain above, even if the data are supplied by third parties, a website operator may still contribute to the content's illegality and thus be liable as a developer.[31] Providing immunity every time a website uses data initially obtained from third parties would eviscerate the exception to section 230 for "develop[ing]" unlawful content "in whole or in part."

---

[29] As *Batzel* pointed out, there can be no meaningful difference between an editor starting with a default rule of publishing all submissions and then manually selecting material to be removed from publication, and a default rule of publishing no submissions and manually selecting material to be published-they are flip sides of precisely the same coin. Batzel, 333 F.3d at 1032 ("The scope of [section 230] immunity cannot turn on whether the publisher approaches the selection process as one of inclusion or removal, as the difference is one of method or degree, not substance.").

[30] The dissent scores a debater's point by noting that the same activity might amount to "development" or not, depending on whether it contributes materially to the illegality of the content. But we are not defining "development" for all purposes; we are defining the term only for purposes of determining whether the defendant is entitled to immunity for a particular act. This definition does not depend on finding substantive liability, but merely requires analyzing the context in which a claim is brought. A finding that a defendant is not immune is quite distinct from finding liability: On remand, Roommate may still assert other defenses to liability under the Fair Housing Act, or argue that its actions do not violate the Fair Housing Act at all. Our holding is limited to a determination that the CDA provides no immunity to Roommate's actions in soliciting and developing the content of its website; whether that content is in fact illegal is a question we leave to the district court.

[31] We disavow any suggestion that Carafano holds an information content provider *automatically* immune so long as the content originated with another information content provider.

We believe a more plausible rationale for the unquestionably correct result in Carafano is this: The allegedly libelous content there—the false implication that Carafano was unchaste—was created and developed entirely by the malevolent user, without prompting or help from the website operator. To be sure, the website provided neutral tools, which the anonymous dastard used to publish the libel, but the website did absolutely nothing to encourage the posting of defamatory content—indeed, the defamatory posting was contrary to the website's express policies. The claim against the website was, in effect, that it failed to review each user-created profile to ensure that it wasn't defamatory. That is precisely the kind of activity for which Congress intended to grant absolution with the passage of section 230. With respect to the defamatory content, the website operator was merely a passive conduit and thus could not be held liable for failing to detect and remove it.[32]

By contrast, Roommate both elicits the allegedly illegal content and makes aggressive use of it in conducting its business. Roommate does not merely provide a framework that could be utilized for proper or improper purposes; rather, Roommate's work in developing the discriminatory questions, discriminatory answers and discriminatory search mechanism is directly related to the alleged illegality of the site. Unlike *Carafano*, where the website operator had nothing to do with the user's decision to enter a celebrity's name and personal information in an otherwise licit dating service, here, Roommate is directly involved with developing and enforcing a system that subjects subscribers to allegedly discriminatory housing practices.

Our ruling today also dovetails with another facet of *Carafano*: The mere fact that an interactive computer service "classifies user characteristics ... does not transform [it] into a 'developer' of the 'underlying misinformation.'" *Carafano*, like *Batzel*, correctly anticipated our common-sense interpretation of the term "develop[ ]" in section 230. Of course, any classification of information, like the sorting of dating profiles by the type of relationship sought in *Carafano*, could be construed as "develop[ment]" under an unduly broad reading of the term. But, once again, such a broad reading would sap section 230 of all meaning.

The salient fact in *Carafano* was that the website's classifications of user characteristics did absolutely nothing to enhance the defamatory sting of the message, to encourage defamation or to make defamation easier: The site provided neutral tools specifically designed to match romantic partners depending on their voluntary inputs. By sharp contrast, Roommate's website is designed to force subscribers to divulge protected characteristics and discriminatory preferences, and to match those who have rooms with those who are looking for rooms based on criteria that appear to be prohibited by the FHA.[33]

---

[32] Section 230 requires us to scrutinize particularly closely any claim that can be boiled down to the failure of an interactive computer service to edit or block user-generated content that it believes was tendered for posting online, as that is the very activity Congress sought to immunize by passing the section.

The dissent coyly suggests that our opinion "sets us apart from" other circuits, carefully avoiding the phrase "inter-circuit conflict." And with good reason: No other circuit has considered a case like ours and none has a case that even arguably conflicts with our holding today. No case cited by the dissent involves active participation by the defendant in the creation or development of the allegedly unlawful content; in each, the interactive computer service provider passively relayed content generated by third parties, just as in *Stratton Oakmont*, and did not design its system around the dissemination of unlawful content.

In Chicago Lawyers' Committee for Civil Rights Under Law, Inc. v. craigslist, Inc., 519 F.3d 666 (7th Cir. 2008), the Seventh Circuit held the online classified website craigslist immune from liability for discriminatory

3. Councils finally argue that Roommate should be held liable for the discriminatory statements displayed in the "Additional Comments" section of profile pages. At the end of the registration process, on a separate page from the other registration steps, Roommate prompts subscribers to "tak[e] a moment to personalize your profile by writing a paragraph or two describing yourself and what you are looking for in a roommate." The subscriber is presented with a blank text box, in which he can type as much or as little about himself as he wishes. Such essays are visible only to paying subscribers.

Subscribers provide a variety of provocative, and often very revealing, answers. The contents range from subscribers who "[p]ref[er] white Male roommates" or require that "[t]he person applying for the room MUST be a BLACK GAY MALE" to those who are "NOT looking for black muslims." Some common themes are a desire to live without "drugs, kids or animals" or "smokers, kids or druggies," while a few subscribers express more particular preferences, such as preferring to live in a home free of "psychos or anyone on mental medication." Some subscribers are just looking for someone who will get along with their significant other[34] or with their most significant Other.[35]

---

housing advertisements submitted by users. Craigslist's service works very much like the "Additional Comments" section of Roommate's website, in that users are given an open text prompt in which to enter any description of the rental property without any structure imposed on their content or any requirement to enter discriminatory information: "Nothing in the service craigslist offers induces anyone to post any particular listing or express a preference for discrimination...." We similarly hold the "Additional Comments" section of Roommate's site immune. Consistent with our opinion, the Seventh Circuit explained the limited scope of section 230(c) immunity. More directly, the Seventh Circuit noted in dicta that "causing a *particular* statement to be made, or perhaps [causing] the *discriminatory content of a statement* " might be sufficient to create liability for a website. (emphasis added). Despite the dissent's attempt to imply the contrary, the Seventh Circuit's opinion is actually in line with our own.

In Universal Communication Systems v. Lycos, Inc., the First Circuit held a message board owner immune under the CDA for defamatory comments posted on a message board. The allegedly defamatory comments were made without any prompting or encouragement by defendant: "[T]here is not even a colorable argument that any misinformation was prompted by Lycos's registration process or its link structure."

Green v. America Online, 318 F.3d 465 (3d Cir. 2003), falls yet farther from the mark. There, AOL was held immune for derogatory comments and malicious software transmitted by other defendants through AOL's "Romance over 30" "chat room." There was no allegation that AOL solicited the content, encouraged users to post harmful content or otherwise had any involvement whatsoever with the harmful content, other than through providing "chat rooms" for general use.

In Ben Ezra, Weinstein, and Co. v. America Online Inc., 206 F.3d 980 (10th Cir. 2000), the Tenth Circuit held AOL immune for relaying inaccurate stock price information it received from other vendors. While AOL undoubtedly participated in the decision to make stock quotations available to members, it did not cause the errors in the stock data, nor did it encourage or solicit others to provide inaccurate data. AOL was immune because "Plaintiff could not identify any evidence indicating Defendant [AOL] developed or created the stock quotation information."

And, finally, in Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997), the Fourth Circuit held AOL immune for yet another set of defamatory and harassing message board postings. Again, AOL did not solicit the harassing content, did not encourage others to post it, and had nothing to do with its creation other than through AOL's role as the provider of a generic message board for general discussions.

[34] "The female we are looking for hopefully wont [sic] mind having a little sexual incounter [sic] with my boyfriend and I [very sic]."

[35] "We are 3 Christian females who Love our Lord Jesus Christ.... We have weekly bible studies and bi-weekly times of fellowship."

Roommate publishes these comments as written.[36] It does not provide any specific guidance as to what the essay should contain, nor does it urge subscribers to input discriminatory preferences. Roommate is not responsible, in whole or in part, for the development of this content, which comes entirely from subscribers and is passively displayed by Roommate. Without reviewing every essay, Roommate would have no way to distinguish unlawful discriminatory preferences from perfectly legitimate statements. Nor can there be any doubt that this information was tendered to Roommate for publication online. This is precisely the kind of situation for which section 230 was designed to provide immunity.

The fact that Roommate encourages subscribers to provide something in response to the prompt is not enough to make it a "develop[er]" of the information under the common-sense interpretation of the term we adopt today. It is entirely consistent with Roommate's business model to have subscribers disclose as much about themselves and their preferences as they are willing to provide. But Roommate does not tell subscribers what kind of information they should or must include as "Additional Comments," and certainly does not encourage or enhance any discriminatory content created by users. Its simple, generic prompt does not make it a developer of the information posted.[37]

Councils argue that—given the context of the discriminatory questions presented earlier in the registration process—the "Additional Comments" prompt impliedly suggests that subscribers should make statements expressing a desire to discriminate on the basis of protected classifications; in other words, Councils allege that, by encouraging some discriminatory preferences, Roommate encourages other discriminatory preferences when it gives subscribers a chance to describe themselves. But the encouragement that bleeds over from one part of the registration process to another is extremely weak, if it exists at all. Such weak encouragement cannot strip a website of its section 230 immunity, lest that immunity be rendered meaningless as a practical matter.[38]

We must keep firmly in mind that this is an immunity statute we are expounding, a provision enacted to protect websites against the evil of liability for failure to remove offensive content. Websites are complicated enterprises, and there will always be close cases where a clever lawyer could argue that something the website operator did encouraged the illegality. Such close cases, we believe, must be resolved in favor of immunity, lest we cut the heart out of section 230 by forcing websites to face death by ten thousand duck-bites, fighting off claims that they promoted or encouraged—or at least tacitly assented to—the illegality of third parties. Where it is very clear that the website directly participates in developing the alleged illegality—as it is clear here with respect to Roommate's questions, answers and the resulting profile pages—immunity will be lost. But in cases of enhancement by implication or development by inference—such as with

[36] It is unclear whether Roommate performs any filtering for obscenity or "spam," but even if it were to perform this kind of minor editing and selection, the outcome would not change.

[37] Nor would Roommate be the developer of discriminatory content if it provided a free-text search that enabled users to find keywords in the "Additional Comments" of others, even if users utilized it to search for discriminatory keywords. Providing neutral tools for navigating websites is fully protected by CDA immunity, absent substantial affirmative conduct on the part of the website creator promoting the use of such tools for unlawful purposes.

[38] It's true that, under a pedantic interpretation of the term "develop," any action by the website—including the mere act of making a text box available to write in—could be seen as "develop[ing]" content. However, we have already rejected such a broad reading of the term "develop" because it would defeat the purpose of section 230.

respect to the "Additional Comments" here—section 230 must be interpreted to protect websites not merely from ultimate liability, but from having to fight costly and protracted legal battles.

The dissent prophesies doom and gloom for countless Internet services, but fails to recognize that we hold part of Roommate's service entirely immune from liability. The search engines the dissent worries about closely resemble the "Additional Comments" section of Roommate's website. Both involve a generic text prompt with no direct encouragement to perform illegal searches or to publish illegal content. We hold Roommate immune and there is no reason to believe that future courts will have any difficulty applying this principle.[39] The message to website operators is clear: If you don't encourage illegal content, or design your website to require users to input illegal content, you will be immune.

We believe that this distinction is consistent with the intent of Congress to preserve the free-flowing nature of Internet speech and commerce without unduly prejudicing the enforcement of other important state and federal laws. When Congress passed section 230 it didn't intend to prevent the enforcement of all laws online; rather, it sought to encourage interactive computer services that provide users *neutral* tools to post content online to police that content without fear that through their "good samaritan ... screening of offensive material," they would become liable for every single message posted by third parties on their website.

* * *

In light of our determination that the CDA does not provide immunity to Roommate for all of the content of its website and email newsletters, we remand for the district court to determine in the first instance whether the alleged actions for which Roommate is not immune violate the Fair Housing Act, 42 U.S.C. § 3604(c).[40] We vacate the dismissal of the state law claims so that the district court may reconsider whether to exercise its supplemental jurisdiction in light of our ruling on the federal claims. We deny Roommate's cross-appeal of the denial of attorneys' fees and costs; Councils prevail on some of their arguments before us so their case is perforce not frivolous.

REVERSED in part, VACATED in part, AFFIRMED in part and REMANDED. NO COSTS.

---

[39] The dissent also accuses us of creating uncertainty that will chill the continued growth of commerce on the Internet. Even looking beyond the fact that the Internet has outgrown its swaddling clothes and no longer needs to be so gently coddled, some degree of uncertainty is inevitable at the edge of any rule of law. Any immunity provision, including section 230, has its limits and there will always be close cases. Our opinion extensively clarifies where that edge lies, and gives far more guidance than our previous cases. While the dissent disagrees about the scope of the immunity, there can be little doubt that website operators today know more about how to conform their conduct to the law than they did yesterday.

However, a larger point remains about the scope of immunity provisions. It's no surprise that defendants want to extend immunity as broadly as possible. We have long dealt with immunity in different, and arguably far more important, contexts—such as qualified immunity for police officers in the line of duty—and observed many defendants argue that the risk of getting a close case wrong is a justification for broader immunity. Accepting such an argument would inevitably lead to an endless broadening of immunity, as every new holding creates its own borderline cases.

[40] We do not address Roommate's claim that its activities are protected by the First Amendment. The district court based its decision entirely on the CDA and we refrain from deciding an issue that the district court has not had the opportunity to evaluate.

McKEOWN, Circuit Judge, with whom RYMER and BEA, Circuit Judges, join, concurring in part and dissenting in part:

The ubiquity of the Internet is undisputed. With more than 1.3 billion Internet users and over 158 million websites in existence, a vast number of them interactive like Google, Yahoo!, Craigslist, MySpace, YouTube, and Facebook, the question of webhost liability is a significant one. On a daily basis, we rely on the tools of cyberspace to help us make, maintain, and rekindle friendships; find places to live, work, eat, and travel; exchange views on topics ranging from terrorism to patriotism; and enlighten ourselves on subjects from "aardvarks to Zoroastrianism."

The majority's unprecedented expansion of liability for Internet service providers threatens to chill the robust development of the Internet that Congress envisioned. The majority condemns Roommate's "search system," a function that is the heart of interactive service providers. My concern is not an empty Chicken Little "sky is falling" alert. By exposing every interactive service provider to liability for sorting, searching, and utilizing the all too familiar drop-down menus, the majority has dramatically altered the landscape of Internet liability. Instead of the "robust" immunity envisioned by Congress, interactive service providers are left scratching their heads and wondering where immunity ends and liability begins.

To promote the unfettered development of the Internet, Congress adopted the Communications Decency Act of 1996 ("CDA"), which provides that interactive computer service providers will not be held legally responsible for publishing information provided by third parties. Even though traditional publishers retain liability for performing essentially equivalent acts in the "non-virtual world," Congress chose to treat interactive service providers differently by immunizing them from liability stemming from sorting, searching, and publishing third-party information. As we explained in *Batzel v. Smith*:

> [Section] 230(c)(1)[ ] overrides the traditional treatment of publishers, distributors, and speakers under statutory and common law. As a matter of policy, "Congress decided not to treat providers of interactive computer services like other information providers such as newspapers, magazines or television and radio stations...." Congress ... has chosen to treat cyberspace differently.

Now, with the stroke of a pen or, more accurately, a few strokes of the keyboard, the majority upends the settled view that interactive service providers enjoy broad immunity when publishing information provided by third parties. Instead, interactive service providers are now joined at the hip with third-party users, and they rise and fall together in liability for Internet sortings and postings.

To be sure, the statute, which was adopted just as the Internet was beginning a surge of popular currency, is not a perfect match against today's technology. The Web 2.0 version is a far cry from web technology in the mid-1990s. Nonetheless, the basic message from Congress has retained its traction, and there should be a high bar to liability for organizing and searching third-party information. The bipartisan view in Congress was that the Internet, as a new form of communication, should not be impeded by the transference of regulations and principles

developed from traditional modes of communication. The majority repeatedly harps that if something is prohibited in the physical world, Congress could not have intended it to be legal in cyberspace. Yet that is precisely the path Congress took with the CDA: the anomaly that a webhost may be immunized for conducting activities in cyberspace that would traditionally be cause for liability is exactly what Congress intended by enacting the CDA.

In the end, the majority offers interactive computer service providers no bright lines and little comfort in finding a home within § 230(c)(1). The result in this case is driven by the distaste for housing discrimination, a laudable endgame were housing the real focus of this appeal. But it is not. I share the majority's view that housing discrimination is a troubling issue. Nevertheless, we should be looking at the housing issue through the lens of the Internet, not from the perspective of traditional publisher liability. Whether § 230(c)(1) trumps the Fair Housing Act ("FHA") is a policy decision for Congress, not us. Congress has spoken: third-party content on the Internet should not be burdened with the traditional legal framework.

I respectfully part company with the majority as to Part 2 of the opinion because the majority has misconstrued the statutory protection under the CDA for Roommate's publishing and sorting of user profiles. The plain language and structure of the CDA unambiguously demonstrate that Congress intended these activities—the collection, organizing, analyzing, searching, and transmitting of third-party content—to be beyond the scope of traditional publisher liability. The majority's decision, which sets us apart from five circuits, contravenes congressional intent and violates the spirit and serendipity of the Internet.

Specifically, the majority's analysis is flawed for three reasons: (1) the opinion conflates the questions of liability under the FHA and immunity under the CDA; (2) the majority rewrites the statute with its definition of "information content provider," labels the search function "information development," and strips interactive service providers of immunity; and (3) the majority's approach undermines the purpose of § 230(c)(1) and has far-reaching practical consequences in the Internet world.

To begin, it is important to recognize what this appeal is not about. At this stage, there has been no determination of liability under the FHA, nor has there been any determination that the questions, answers or even the existence of Roommate's website violate the FHA. The FHA is a complicated statute and there may well be room for potential roommates to select who they want to live with, e.g., a tidy accountant wanting a tidy professional roommate, a collegiate male requesting a male roommate, an observant Jew needing a house with a kosher kitchen, or a devout, single, religious female preferring not to have a male housemate. It also bears noting that even if Roommate is immune under the CDA, the issue of user liability for allegedly discriminatory preferences is a separate question.

By offering up inflammatory examples, the majority's opinion screams "discrimination." The hazard is, of course, that the question of discrimination has not yet been litigated. In dissenting, I do not condone housing discrimination or endorse unlawful discriminatory roommate selection practices; I simply underscore that the merits of the FHA claim are not before us. However, one would not divine this posture from the majority's opinion, which is infused with condemnation of Roommate's users' practices. To mix and match, as does the majority, the alleged

unlawfulness of the information with the question of webhost immunity is to rewrite the statute….

The entire opinion links Roommate's ostensibly reprehensible conduct (and that of its users) with an unprecedented interpretation of the CDA's immunity provision. The majority condemns Roommate for soliciting illegal content, but there has been no determination that Roommate's questions or standardized answers are illegal. Instead of foreshadowing a ruling on the FHA, the opinion should be confined to the issue before us—application of § 230(c)(1) to Roommate. The district court has not yet ruled on the merits of the FHA claim and neither should we.

The Statute

With this background in mind, I first turn to the text of the statute. Section 230 begins with a detailed recitation of findings and policy reasons for the statute. Congress expressly found that the "Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity," and that "[i]ncreasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services." Congress declared that "[i]t is the policy of the United States to ... promote the continued development of the Internet and other interactive computer services and other interactive media."

Unlike some statutes, subsections (a) and (b) set out in clear terms the congressional findings and policies underlying the statute. For this reason, it strikes me as odd that the majority begins, not with the statute and these express findings, but with legislative history. Granted, Congress was prompted by several cases, particularly the *Prodigy* case, to take action to protect interactive service providers. But that case does not cabin the scope of the statute, and the background leading up to enactment of the CDA is no substitute for the language of the statute itself.

Section 230(c), the heart of this case, is entitled "Protection for 'good samaritan' blocking and screening of offensive material[.]" The substantive language of the statute itself is not so limited….

Since it was first addressed in 1997 in *Zeran*, this section has been interpreted by the courts as providing webhost "immunity," although to be more precise, it provides a safe haven for interactive computer service providers by removing them from the traditional liabilities attached to speakers and publishers.

We have characterized this immunity under § 230(c)(1) as "quite robust." Five of our sister circuits have similarly embraced this robust view of immunity by providing differential treatment to interactive service providers….

Courts deciding the question of § 230(c)(1) immunity "do not write on a blank slate." Even though rapid developments in technology have made webhosts increasingly adept at searching and displaying third-party information, reviewing courts have, in the twelve years since the CDA's enactment, "adopt[ed] a relatively expansive definition of 'interactive computer service' and a relatively restrictive definition of 'information content provider.'" As long as information

is provided by a third party, webhosts are immune from liability for publishing "ads for housing, auctions of paintings that may have been stolen by Nazis, biting comments about steroids in baseball, efforts to verify the truth of politicians' promises, and everything else that third parties may post on a web site." We have underscored that this broad grant of webhost immunity gives effect to Congress's stated goals "to promote the continued development of the Internet and other interactive computer services" and "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services."

Application of § 230(c)(1) to Roommate's Website

Because our focus is on the term "information content provider," and what it means to create or develop information, it is worth detailing exactly how the website operates, what information is at issue and who provides it. The roommate matching process involves three categories of data: About Me or Household Description; Roommate Preferences; and Comments.

To become a member of Roommates.com, a user must complete a personal profile by selecting answers from drop-down menus or checking off boxes on the screen. The profile includes "location" information (e.g., city and state, region of the city, and data about the surrounding neighborhood); details about the residence (e.g., the total number of bedrooms and bathrooms in the home, and amenities such as air conditioning, wheelchair access, high-speed Internet, or parking), and the "rental details" (e.g., monthly rent charged, lease period, and availability). The last section of the profile is the "Household Description" section, which includes the total number of occupants in the home, their age range, gender, occupation, level of cleanliness, whether they are smokers, and whether children or pets are present.

The remaining sections of the registration process are completely optional; a user who skips them has created a profile based on the information already provided. At his option, the user may select an emoticon to describe the "household character," and may upload images of the room or residence. Next, users may, at their option, specify characteristics desired in a potential roommate, such as a preferred age range, gender, and level of cleanliness. If nothing is selected, all options are included. The final step in the registration process, which is also optional, is the "Comments" section, in which users are presented with a blank text box in which they may write whatever they like, to be published with their member profiles.

Users may choose an optional "custom search" of user profiles based on criteria that they specify, like the amount of monthly rent or distance from a preferred city. Based on the information provided by users during the registration process, Roommate's automated system then searches and matches potential roommates. Roommate's Terms of Service provide in part, "You understand that we do not provide the information on the site and that all publicly posted or privately transmitted information, data, text, photographs, graphics, messages, or other materials ('Content') are the sole responsibility of the person from which such Content originated."

Roommate's users are "information content providers" because they are responsible for creating the information in their user profiles and, at their option—not the website's choice—in expressing preferences as to roommate characteristics. The critical question is whether

Roommate is itself an "information content provider," such that it cannot claim that the information at issue was "provided by another information content provider." A close reading of the statute leads to the conclusion that Roommate is not an information content provider for two reasons: (1) providing a drop-down menu does not constitute "creating" or "developing" information; and (2) the structure and text of the statute make plain that Congress intended to immunize Roommate's sorting, displaying, and transmitting of third-party information.

Roommate neither "creates" nor "develops" the information that is challenged by the Councils, i.e., the information provided by the users as to their protected characteristics and the preferences expressed as to roommate characteristics. All Roommate does is to provide a form with options for standardized answers. Listing categories such as geographic location, cleanliness, gender and number of occupants, and transmitting to users profiles of other users whose expressed information matches their expressed preferences, can hardly be said to be creating or developing information. Even adding standardized options does not "develop" information. Roommate, with its prompts, is merely "selecting material for publication," which we have stated does not constitute the "development" of information. The profile is created solely by the user, not the provider of the interactive website. Indeed, without user participation, there is no information at all. The drop-down menu is simply a precategorization of user information before the electronic sorting and displaying that takes place via an algorithm. If a user has identified herself as a non-smoker and another has expressed a preference for a non-smoking roommate, Roommate's sorting and matching of user information are no different than that performed by a generic search engine.

Displaying the prompt "Gender" and offering the list of choices, "Straight male; Gay male; Straight female; Gay female" does not develop the information, "I am a Gay male." The user has identified himself as such and provided that information to Roommate to publish. Thus, the user is the sole creator of that information; no "development" has occurred. In the same vein, presenting the user with a "Preferences" section and drop-down menus of options does not "develop" a user's preference for a non-smoking roommate. As we stated in Carafano, the "actual profile 'information' consist[s] of the particular options chosen" by the user, such that Roommate is not "responsible, even in part, for associating certain multiple choice responses with a set of [ ] characteristics."

The thrust of the majority's proclamation that Roommate is "developing" the information that it publishes, sorts, and transmits is as follows: "[W]e interpret the term 'development' as referring not merely to augmenting the content generally, but to materially contributing to its unlawfulness." This definition is original to say the least and springs forth untethered to anything in the statute.

The majority's definition of "development" epitomizes its consistent collapse of substantive liability with the issue of immunity. Where in the statute does Congress say anything about unlawfulness? Whether Roommate is entitled to immunity for publishing and sorting profiles is wholly distinct from whether Roommate may be liable for violations of the FHA. Immunity has meaning only when there is something to be immune from, whether a disease or the violation of a law. It would be nonsense to claim to be immune only from the innocuous. But the majority's immunity analysis is built on substantive liability: to the majority, CDA immunity depends on

whether a webhost materially contributed to the unlawfulness of the information. Whether the information at issue is unlawful and whether the webhost has contributed to its unlawfulness are issues analytically independent of the determination of immunity. Grasping at straws to distinguish Roommate from other interactive websites such as Google and Yahoo!, the majority repeatedly gestures to Roommate's potential substantive liability as sufficient reason to disturb its immunity. But our task is to determine whether the question of substantive liability may be reached in the first place.

Keep in mind that "unlawfulness" would include not only purported statutory violations but also potential defamatory statements. The irony is that the majority would have us determine "guilt" or liability in order to decide whether immunity is available. This upside-down approach would knock out even the narrowest immunity offered under § 230(c)—immunity for defamation as a publisher or speaker.

Another flaw in the majority's approach is that it fails to account for all of the other information allegedly developed by the webhost. For purposes of determining whether Roommate is an information content provider vis-a-vis the profiles, the inquiry about geography and the inquiry about gender should stand on the same footing. Both are single word prompts followed by a drop-down menu of options. If a prompt about gender constitutes development, then so too does the prompt about geography. And therein lies the rub.

Millions of websites use prompts and drop-down menus. Inquiries range from what credit card you want to use and consumer satisfaction surveys asking about age, sex and household income, to dating sites, e.g., match.com, sites lambasting corporate practices, e.g., ripoffreports.com, and sites that allow truckers to link up with available loads, e.g., getloaded.com. Some of these sites are innocuous while others may not be. Some may solicit illegal information; others may not. But that is not the point. The majority's definition of "development" would transform every interactive site into an information content provider and the result would render illusory any immunity under § 230(c). Virtually every site could be responsible in part for developing content.

For example, the majority purports to carve out a place for Google and other search engines. But the modern Google is more than a match engine: it ranks search results, provides prompts beyond what the user enters, and answers questions. In contrast, Roommate is a straight match service that searches information and criteria provided by the user, not Roommate. It should be afforded no less protection than Google, Yahoo!, or other search engines.

The majority then argues that "providing *neutral* tools to carry out what may be unlawful or illicit searches does not amount to 'development.'" But this effort to distinguish Google, Yahoo!, and other search engines from Roommate is unavailing. Under the majority's definition of "development," these search engines are equivalent to Roommate. Google "encourages" or "contributes" (the majority's catch phrases) to the unlawfulness by offering search tools that allow the user to perform an allegedly unlawful match. If a user types into Google's search box, "looking for a single, Christian, female roommate," and Google displays responsive listings, Google is surely "materially contributing to the alleged unlawfulness" of information created by third parties, by publishing their intention to discriminate on the basis of protected

characteristics. In the defamation arena, a webhost's publication of a defamatory statement "materially contributes" to its unlawfulness, as publication to third parties is an element of the offense. At bottom, the majority's definition of "development" can be tucked in, let out, or hemmed up to fit almost any search engine, creating tremendous uncertainty in an area where Congress expected predictability.

"Development" is not without meaning. In *Batzel*, we hinted that the "development of information" that transforms one into an "information content provider" is "something more substantial than merely editing portions of an email and selecting material for publication." We did not flesh out further the meaning of "development" because the editor's alterations of an email message and decision to publish it did not constitute "development."

Because the statute does not define "development," we should give the term its ordinary meaning. "Development" is defined in Webster's Dictionary as a "gradual advance or growth through progressive changes." The multiple uses of "development" and "develop" in other provisions of § 230 give texture to the definition of "development," and further expose the folly of the majority's ungrounded definition. Defining "development" in this way keeps intact the settled rule that the CDA immunizes a webhost who exercises a publisher's "traditional editorial functions—such as deciding whether to publish, withdraw, postpone, or alter content."[11]

Applying the plain meaning of "development" to Roommate's sorting and transmitting of third-party information demonstrates that it was not transformed into an "information content provider." In searching, sorting, and transmitting information, Roommate made no changes to the information provided to it by users. Even having notice that users may be using its site to make discriminatory statements is not sufficient to invade Roommate's immunity.

The majority blusters that Roommate develops information, because it "requir[es] subscribers to provide the information as a condition of accessing its services," and "designed its search system so it would steer users based on the preferences and personal characteristics that Roommate itself forces subscribers to disclose." But the majority, without looking back, races past the plain language of the statute. That Roommate requires users to answer a set of prompts to identify characteristics about themselves does not change the fact that the users have furnished this information to Roommate for Roommate to publish in their profiles. Nor do Roommate's prompts alter the fact that users have chosen to select characteristics that they find desirable in

[11] The majority's notion of using a different definition of "development" digs the majority into a deeper hole. For example, adopting the Wikipedia definition of "content development"—"the process of researching, writing, gathering, organizing and editing information for publication on web sites"—would run us smack into the sphere of Congressionally conferred immunity. Both our circuit and others have steadfastly maintained that activities such as organizing or editing information are traditional editorial functions that fall within the scope of CDA immunity. Likewise, an alternative definition of "development" from Webster's such as "a making usable or available" sweeps too broadly, as "making usable or available" is precisely what Google and Craigslist do. In an effort to cabin the reach of the opinion, the majority again goes back to whether the content is legal, i.e., a dating website that requires sex, race, religion, or marital status is legal because it is legal to discriminate in dating. Of course this approach ignores whether the claim may be one in tort, such as defamation, rather than a statutory discrimination claim. And, this circularity also circumvents the plain language of the statute. Interestingly, the majority has no problem offering up potentially suitable definitions of "development" by turning to dictionaries, but it fails to explain why, and from where, it plucked its definition of "development" as "materially contributing to [the] alleged unlawfulness" of content.

potential roommates, and have directed Roommate to search and compile results responsive to their requests. Moreover, tagging Roommate with liability for the design of its search system is dangerous precedent for analyzing future Internet cases.

Even if Roommate's prompts and drop-down menus could be construed to seek out, or encourage, information from users, the CDA does not withhold immunity for the encouragement or solicitation of information. The CDA does not countenance an exception for the solicitation or encouragement of information provided by users.

A number of district courts have recently encountered the claim that an interactive website's solicitation of information, by requiring user selection of content from drop-down menus, transformed it into an information content provider. Unsurprisingly, these courts reached the same commonsense solution that I reach here: § 230(c)(1) immunizes the interactive service provider. Simply supplying a list of options from which a user must select options "is minor and passive participation" that does not defeat CDA immunity.

Carafano presented circumstances virtually indistinguishable from those before us, yet the majority comes to the exact opposite conclusion here in denying immunity for sorting and matching third-party information provided in response to webhost prompts. The website in *Carafano*, an online dating service named Matchmaker.com, asked its users sixty-two detailed questions and matched users according to their responses. We held that § 230(c)(1) immunized the dating service, and flatly rejected the proposition that matching, sorting, and publishing user information in response to webhost prompts abrogated CDA immunity. A provider's "decision to structure the information provided by users," which enables the provider to "offer additional features, such as 'matching' profiles with similar characteristics or highly structured searches based on combinations of multiple choice questions," ultimately "promotes the expressed Congressional policy 'to promote the continued development of the Internet and other interactive computer services.'" Now the majority narrows *Carafano* on the basis that Matchmaker did not prompt the allegedly libelous information that was provided by a third party. But the majority makes this distinction without any language in the statute supporting the consideration of the webhost's prompting or solicitation.

The structure of the statute also supports my view that Congress intended to immunize Roommate's sorting and publishing of user profiles. An "interactive computer service" is defined to include an "access software provider." The statute defines an "access software provider" as one that provides "enabling tools" to "filter," "screen," "pick," "choose," "analyze," "digest," "search," "forward," "organize," and "reorganize" content.

By providing a definition for "access software provider" that is distinct from the definition of an "information content provider," and withholding immunity for "information content providers," the statute makes resoundingly clear that packaging, sorting, or publishing third-party information are not the kind of activities that Congress associated with "information content providers." Yet these activities describe exactly what Roommate does through the publication and distribution of user profiles: Roommate "receives," "filters," "digests," and "analyzes" the information provided by users in response to its registration prompts, and then "transmits," "organizes," and "forwards" that information to users in the form of uniformly organized

profiles. Roommate is performing tasks that Congress recognized as typical of entities that it intended to immunize.

Finally, consider the logical disconnect of the majority's opinion. The majority writes—and I agree—that the open-ended Comments section contains only third-party content. But if Roommate's search function permits sorting by key words such as children or gender, the majority would label Roommate's use of such criteria as a "discriminatory filtering process."

At a minimum, the CDA protects the search criteria employed by websites and does not equate tools that "filter," "screen," "pick," "choose," "analyze," "digest," "search," "forward," "organize," and "reorganize" with the "creation or development" of information.

Ramifications of the Majority Opinion

I am troubled by the consequences that the majority's conclusion poses for the ever-expanding Internet community. The unwise narrowing of our precedent, coupled with the mixing and matching of CDA immunity with substantive liability, make it exceedingly difficult for website providers to know whether their activities will be considered immune under the CDA. We got it right in *Carafano*, that "[u]nder § 230(c) ... so long as a third party willingly provides the essential published content, the interactive service provider receives full immunity regardless of the specific editing or selection process."

Significantly, § 230(e) expressly exempts from its scope certain areas of law, such as intellectual property law and federal criminal laws. Thus, for example, a webhost may still be liable as a publisher or speaker of third-party information that is alleged to infringe a copyright. Notably, the CDA does not exempt the FHA and a host of other federal statutes from its scope. The FHA existed at the time of the CDA's enactment, yet Congress did not add it to the list of specifically enumerated laws for which publisher and speaker liability was left intact. The absence of a statutory exemption suggests that Congress did not intend to provide special case status to the FHA in connection with immunity under the CDA.

Anticipating the morphing of the Internet and the limits of creative genius and entrepreneurship that fuel its development is virtually impossible. However, Congress explicitly drafted the law to permit this unfettered development of the Internet. Had Congress discovered that, over time, courts across the country have created more expansive immunity than it originally envisioned under the CDA, Congress could have amended the law. But it has not. In fact, just six years ago, Congress approved of the broad immunity that courts have uniformly accorded interactive webhosts under § 230(c).

In 2002, Congress passed the "Dot Kids Implementation and Efficiency Act," which established a new "kids.us" domain for material that is safe for children. Congress stated that the statutory protections of § 230(c) were extended to certain entities that operated within the new domain. The Committee Report that accompanied the statute declared:

> The Committee notes that ISPs have successfully defended many lawsuits using section 230(c). *The courts have correctly interpreted section 230(c)*, which was

> aimed at protecting against liability for such claims as negligence (See, e.g., Doe v. America Online, 783 So.2d 1010 (Fla. 2001)) and defamation (Ben Ezra, Weinstein, and Co. v. America Online, 206 F.3d 980 (2000); Zeran v. America Online, 129 F.3d 327 (1997)). The Committee intends these interpretations of section 230(c) to be equally applicable to those entities covered by H.R. 3833.

H.R. REP. No. 107-449 (emphasis added). These statements "reflect the Committee's intent that the existing statutory construction," i.e., broad immunity for interactive webhosts, "be maintained in a new legislative context." This express Congressional approval of the courts' interpretation of § 230(c)(1), six years after its enactment, advises us to stay the course of "robust" webhost immunity.

The consequences of the majority's interpretation are far-reaching. Its position will chill speech on the Internet and impede "the continued development of the Internet and other interactive computer services and other interactive media." To the extent the majority strips immunity because of sorting, channeling, and categorizing functions, it guts the heart of § 230(c)(1) immunity. Countless websites operate just like Roommate: they organize information provided by their users into a standardized format, and provide structured searches to help users find information. These sites, and their attendant display, search, and inquiry tools, are an indispensable part of the Internet tool box. Putting a lid on the sorting and searching functions of interactive websites stifles the core of their services.

To the extent the majority strips immunity because the information or query may be illegal under some statute or federal law, this circumstance puts the webhost in the role of a policeman for the laws of the fifty states and the federal system. There are not enough Net Nannies in cyberspace to implement this restriction, and the burden of filtering content would be unfathomable.

To the extent the majority strips immunity because a site solicits or actively encourages content, the result is a direct restriction on the free exchange of ideas and information on the Internet. As noted in the amici curiae brief of the news organizations, online news organization routinely solicit third-party information. Were the websites to face host liability for this content, they "would have no choice but to severely limit its use" and "[s]heer economics would dictate that vast quantities of valuable information be eliminated from websites."

To the extent the majority strips immunity because a website "materially contributed" to the content or output of a website by "specialization" of content, this approach would essentially swallow the immunity provision. The combination of solicitation, sorting, and potential for liability would put virtually every interactive website in this category. Having a website directed to Christians, Muslims, gays, disabled veterans, or childless couples could land the website provider in hot water.[14]

Because the statute itself is cumbersome to interpret in light of today's Internet architecture, and because the decision today will ripple through the billions of web pages already online, and the countless pages to come in the future, I would take a cautious, careful, and precise approach to

[14] It is no surprise that there are countless specialized roommate sites. See, e.g., http://islam.tc/housing/index.php, http://christian-roommates.com, and http://prideroommates.com.

the restriction of immunity, not the broad swath cut by the majority. I respectfully dissent and would affirm the district court's judgment that Roommate is entitled to immunity under § 230(c)(1) of the CDA, subject to examination of whether the bare inquiry itself is unlawful.

16 C.F.R. Part 312—Children's Online Privacy Protection Rule

§ 312.2 Definitions.

Child means an individual under the age of 13.

Collects or collection means the gathering of any personal information from a child by any means, including but not limited to:

(a) Requesting that children submit personal information online;

(b) Enabling children to make personal information publicly available through a chat room, message board, or other means, except where the operator deletes all individually identifiable information from postings by children before they are made public, and also deletes such information from the operator's records; or

(c) The passive tracking or use of any identifying code linked to an individual, such as a cookie.

Commission means the Federal Trade Commission.

Delete means to remove personal information such that it is not maintained in retrievable form and cannot be retrieved in the normal course of business.

Disclosure means, with respect to personal information:

(a) The release of personal information collected from a child in identifiable form by an operator for any purpose, except where an operator provides such information to a person who provides support for the internal operations of the website or online service and who does not disclose or use that information for any other purpose. For purposes of this definition:

(1) *Release of personal information* means the sharing, selling, renting, or any other means of providing personal information to any third party, and

(2) *Support for the internal operations of the website or online service* means those activities necessary to maintain the technical functioning of the website or online service, or to fulfill a request of a child as permitted by §312.5(c)(2) and (3); or

(b) Making personal information collected from a child by an operator publicly available in identifiable form, by any means, including by a public posting through the Internet, or through a personal home page posted on a website or online service; a pen pal service; an electronic mail service; a message board; or a chat room.

Federal agency means an agency, as that term is defined in Section 551(1) of title 5, United States Code.

Internet means collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire, radio, or other methods of transmission.

Online contact information means an e-mail address or any other substantially similar identifier that permits direct contact with a person online.

Operator means any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained, where such website or online service is operated for commercial purposes, including any person offering products or services for sale through that website or online service, involving commerce:

(a) Among the several States or with 1 or more foreign nations;

(b) In any territory of the United States or in the District of Columbia, or between any such territory and

(1) Another such territory, or

(2) Any State or foreign nation; or

(c) Between the District of Columbia and any State, territory, or foreign nation. This definition does not include any nonprofit entity that would otherwise be exempt from coverage under Section 5 of the Federal Trade Commission Act (15 U.S.C. 45).

Parent includes a legal guardian.

Person means any individual, partnership, corporation, trust, estate, cooperative, association, or other entity.

Personal information means individually identifiable information about an individual collected online, including:

(a) A first and last name;

(b) A home or other physical address including street name and name of a city or town;

(c) An e-mail address or other online contact information, including but not limited to an instant messaging user identifier, or a screen name that reveals an individual's e-mail address;

(d) A telephone number;

(e) A Social Security number;

(f) A persistent identifier, such as a customer number held in a cookie or a processor serial number, where such identifier is associated with individually identifiable information; or a combination of a last name or photograph of the individual with other information such that the combination permits physical or online contacting; or

(g) Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.

Third party means any person who is not:

(a) An operator with respect to the collection or maintenance of personal information on the website or online service; or

(b) A person who provides support for the internal operations of the website or online service and who does not use or disclose information protected under this part for any other purpose.

Obtaining *verifiable consent* means making any reasonable effort (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child:

(a) Receives notice of the operator's personal information collection, use, and disclosure practices; and

(b) Authorizes any collection, use, and/or disclosure of the personal information.

Website or online service directed to children means a commercial website or online service, or portion thereof, that is targeted to children. Provided, however, that a commercial website or online service, or a portion thereof, shall not be deemed directed to children solely because it refers or links to a commercial website or online service directed to children by using information location tools, including a directory, index, reference, pointer, or hypertext link. In determining whether a commercial website or online service, or a portion thereof, is targeted to children, the Commission will consider its subject matter, visual or audio content, age of models, language or other characteristics of the website or online service, as well as whether advertising promoting or appearing on the website or online service is directed to children. The Commission

will also consider competent and reliable empirical evidence regarding audience composition; evidence regarding the intended audience; and whether a site uses animated characters and/or child-oriented activities and incentives.

§ 312.3 Regulation of unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.

General requirements. It shall be unlawful for any operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under this part. Generally, under this part, an operator must:

(a) Provide notice on the website or online service of what information it collects from children, how it uses such information, and its disclosure practices for such information (§312.4(b));

(b) Obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children (§312.5);

(c) Provide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance (§312.6);

(d) Not condition a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity (§312.7); and

(e) Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children (§312.8).

§ 312.4 Notice.

(a) *General principles of notice*. All notices under §§312.3(a) and 312.5 must be clearly and understandably written, be complete, and must contain no unrelated, confusing, or contradictory materials.

(b) *Notice on the website or online service*. Under §312.3(a), an operator of a website or online service directed to children must post a link to a notice of its information practices with regard to children on the home page of its website or online service and at each area on the website or online service where personal information is collected from children. An operator of a general audience website or online service that has a separate children's area or site must post a link to a notice of its information practices with regard to children on the home page of the children's area.

(1) *Placement of the notice*.

(i) The link to the notice must be clearly labeled as a notice of the website or online service's information practices with regard to children;

(ii) The link to the notice must be placed in a clear and prominent place and manner on the home page of the website or online service; and

(iii) The link to the notice must be placed in a clear and prominent place and manner at each area on the website or online service where children directly provide, or are asked to provide, personal information, and in close proximity to the requests for information in each such area.

(2) *Content of the notice*. To be complete, the notice of the website or online service's information practices must state the following:

(i) The name, address, telephone number, and e-mail address of all operators collecting or maintaining personal information from children through the website or online service. *Provided that*: the operators of a website or online service may list the name, address, phone number, and e-mail address of one operator who will respond to all inquiries from parents concerning the operators' privacy policies and use of children's information, as long as the names of all the operators collecting or maintaining personal information from children through the website or online service are also listed in the notice;

(ii) The types of personal information collected from children and whether the personal information is collected directly or passively;

(iii) How such personal information is or may be used by the operator(s), including but not limited to fulfillment of a requested transaction, recordkeeping, marketing back to the child, or making it publicly available through a chat room or by other means;

(iv) Whether personal information is disclosed to third parties, and if so, the types of business in which such third parties are engaged, and the general purposes for which such information is used; whether those third parties have agreed to maintain the confidentiality, security, and integrity of the personal information they obtain from the operator; and that the parent has the option to consent to the collection and use of their child's personal information without consenting to the disclosure of that information to third parties;

(v) That the operator is prohibited from conditioning a child's participation in an activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity; and

(vi) That the parent can review and have deleted the child's personal information, and refuse to permit further collection or use of the child's information, and state the procedures for doing so.

(c) *Notice to a parent*. Under §312.5, an operator must make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives notice of the operator's practices with regard to the collection, use, and/or disclosure of the child's personal information, including notice of any material change in the collection, use, and/or disclosure practices to which the parent has previously consented.

(1) *Content of the notice to the parent.*

(i) All notices must state the following:

(A) That the operator wishes to collect personal information from the child;

(B) The information set forth in paragraph (b) of this section.

(ii) In the case of a notice to obtain verifiable parental consent under §312.5(a), the notice must also state that the parent's consent is required for the collection, use, and/or disclosure of such information, and state the means by which the parent can provide verifiable consent to the collection of information.

(iii) In the case of a notice under the exception in §312.5(c)(3), the notice must also state the following:

(A) That the operator has collected the child's e-mail address or other online contact information to respond to the child's request for information and that the requested information will require more than one contact with the child;

(B) That the parent may refuse to permit further contact with the child and require the deletion of the information, and how the parent can do so; and

(C) That if the parent fails to respond to the notice, the operator may use the information for the purpose(s) stated in the notice.

(iv) In the case of a notice under the exception in §312.5(c)(4), the notice must also state the following:

(A) That the operator has collected the child's name and e-mail address or other online contact information to protect the safety of the child participating on the website or online service;

(B) That the parent may refuse to permit the use of the information and require the deletion of the information, and how the parent can do so; and

(C) That if the parent fails to respond to the notice, the operator may use the information for the purpose stated in the notice.

§ 312.5 Parental consent.

(a) *General requirements.*

(1) An operator is required to obtain verifiable parental consent before any collection, use, and/or disclosure of personal information from children, including consent to any material change in the collection, use, and/or disclosure practices to which the parent has previously consented.

(2) An operator must give the parent the option to consent to the collection and use of the child's personal information without consenting to disclosure of his or her personal information to third parties.

(b) *Mechanisms for verifiable parental consent.*

(1) An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent.

(2) Methods to obtain verifiable parental consent that satisfy the requirements of this paragraph include: providing a consent form to be signed by the parent and returned to the operator by postal mail or facsimile; requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free telephone number staffed by trained personnel; using a digital certificate that uses public key technology; and using e-mail accompanied by a PIN or password obtained through one of the verification methods listed in this paragraph. *Provided that*: Until the Commission otherwise determines, methods to obtain verifiable parental consent for uses of information other than the "disclosures" defined by §312.2 may also include use of e-mail coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: sending a confirmatory e-mail to the parent following receipt of consent; or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. Operators

who use such methods must provide notice that the parent can revoke any consent given in response to the earlier e-mail.

(c) *Exceptions to prior parental consent*. Verifiable parental consent is required prior to any collection, use and/or disclosure of personal information from a child except as set forth in this paragraph. The exceptions to prior parental consent are as follows:

(1) Where the operator collects the name or online contact information of a parent or child to be used for the sole purpose of obtaining parental consent or providing notice under §312.4. If the operator has not obtained parental consent after a reasonable time from the date of the information collection, the operator must delete such information from its records;

(2) Where the operator collects online contact information from a child for the sole purpose of responding directly on a one-time basis to a specific request from the child, and where such information is not used to recontact the child and is deleted by the operator from its records;

(3) Where the operator collects online contact information from a child to be used to respond directly more than once to a specific request from the child, and where such information is not used for any other purpose. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that a parent receives notice and has the opportunity to request that the operator make no further use of the information, as described in §312.4(c), immediately after the initial response and before making any additional response to the child. Mechanisms to provide such notice include, but are not limited to, sending the notice by postal mail or sending the notice to the parent's e-mail address, but do not include asking a child to print a notice form or sending an e-mail to the child;

(4) Where the operator collects a child's name and online contact information to the extent reasonably necessary to protect the safety of a child participant on the website or online service, and the operator uses reasonable efforts to provide a parent notice as described in §312.4(c), where such information is:

(i) Used for the sole purpose of protecting the child's safety;

(ii) Not used to recontact the child or for any other purpose;

(iii) Not disclosed on the website or online service; and

(5) Where the operator collects a child's name and online contact information and such information is not used for any other purpose, to the extent reasonably necessary:

(i) To protect the security or integrity of its website or online service;

(ii) To take precautions against liability;

(iii) To respond to judicial process; or

(iv) To the extent permitted under other provisions of law, to provide information to law enforcement agencies or for an investigation on a matter related to public safety.

§ 312.6 Right of parent to review personal information provided by a child.

(a) Upon request of a parent whose child has provided personal information to a website or online service, the operator of that website or online service is required to provide to that parent the following:

(1) A description of the specific types or categories of personal information collected from children by the operator, such as name, address, telephone number, e-mail address, hobbies, and extracurricular activities;

(2) The opportunity at any time to refuse to permit the operator's further use or future online collection of personal information from that child, and to direct the operator to delete the child's personal information; and

(3) Notwithstanding any other provision of law, a means of reviewing any personal information collected from the child. The means employed by the operator to carry out this provision must:

(i) Ensure that the requestor is a parent of that child, taking into account available technology; and

(ii) Not be unduly burdensome to the parent.

(b) Neither an operator nor the operator's agent shall be held liable under any Federal or State law for any disclosure made in good faith and following reasonable procedures in responding to a request for disclosure of personal information under this section.

(c) Subject to the limitations set forth in §312.7, an operator may terminate any service provided to a child whose parent has refused, under paragraph (a)(2) of this section, to permit the operator's further use or collection of personal information from his or her child or has directed the operator to delete the child's personal information.

§ 312.7 Prohibition against conditioning a child's participation on collection of personal information.

An operator is prohibited from conditioning a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity.

§ 312.8 Confidentiality, security, and integrity of personal information collected from children.

The operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

§ 312.9 Enforcement.

Subject to sections 6503 and 6505 of the Children's Online Privacy Protection Act of 1998, a violation of a regulation prescribed under section 6502 (a) of this Act shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

§ 312.10 Safe harbors.

(a) In general. An operator will be deemed to be in compliance with the requirements of this part if that operator complies with self-regulatory guidelines, issued by representatives of the marketing or online industries, or by other persons, that, after notice and comment, are approved by the Commission….

In re Pharmatrak, Inc., 329 F.3d 9 (1st Cir. 2003).
Lynch, Circuit Judge.

This case raises important questions about the scope of privacy protection afforded internet users under the Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2511, 2520.

In sum, pharmaceutical companies invited users to visit their websites to learn about their drugs and to obtain rebates. An enterprising company, Pharmatrak, sold a service, called "NETcompare," to these pharmaceutical companies. That service accessed information about the internet users and collected certain information meant to permit the pharmaceutical companies to do intra-industry comparisons of website traffic and usage. Most of the pharmaceutical companies were emphatic that they did not want personal or identifying data about their web site users to be collected. In connection with their contracting to use NETcompare, they sought and received assurances from Pharmatrak that such data collection would not occur. As it turned out, some such personal and identifying data was found, using easily customized search programs, on Pharmatrak's computers. Plaintiffs, on behalf of the purported class of internet users whose data Pharmatrak collected, sued both Pharmatrak and the pharmaceutical companies asserting, inter alia, that they intercepted electronic communications without consent, in violation of the ECPA.

The district court entered summary judgment for defendants on the basis that Pharmatrak's activities fell within an exception to the statute where one party consents to an interception. The court found the client pharmaceutical companies had consented by contracting with Pharmatrak and so this protected Pharmatrak. The plaintiffs dismissed all ECPA claims as to the pharmaceutical companies. This appeal concerns only the claim that Pharmatrak violated Title I of the ECPA.

We hold that the district court incorrectly interpreted the "consent" exception to the ECPA; we also hold that Pharmatrak "intercepted" the communication under the statute. We reverse and remand for further proceedings. This does not mean that plaintiffs' case will prevail: there remain issues which should be addressed on remand, particularly as to whether defendant's conduct was intentional within the meaning of the ECPA.

I.

Pharmatrak provided its NETcompare service to pharmaceutical companies including American Home Products, Pharmacia, SmithKline Beecham, Pfizer, and Novartis from approximately June 1998 to November 2000. The pharmaceutical clients terminated their contracts with Pharmatrak shortly after this lawsuit was filed in August 2000. As a result, Pharmatrak was forced to cease its operations by December 1, 2000.

NETcompare was marketed as a tool that would allow a company to compare traffic on and usage of different parts of its website with the same information from its competitors' websites. The key advantage of NETcompare over off-the-shelf software was its capacity to allow each client to compare its performance with that of other clients from the same industry.

NETcompare was designed to record the webpages a user viewed at clients' websites; how long the user spent on each webpage; the visitor's path through the site (including her points of entry and exit); the visitor's IP address; and, for later versions, the webpage the user viewed immediately before arriving at the client's site (i.e., the "referrer URL"). This information-gathering was not visible to users of the pharmaceutical clients' websites. According to Wes Sonnenreich, former Chief Technology Officer of Pharmatrak, and Timothy W. Macinta, former Managing Director for Technology of Pharmatrak, NETcompare was not designed to collect any personal information whatsoever.

NETcompare operated as follows. A pharmaceutical client installed NETcompare by adding five to ten lines of HTML code to each webpage it wished to track and configuring the pages to interface with Pharmatrak's technology. When a user visited the website of a Pharmatrak client, Pharmatrak's HTML code instructed the user's computer to contact Pharmatrak's web server and retrieve from it a tiny, invisible graphic image known as a "clear GIF" (or a "web bug"). The purpose of the clear GIF was to cause the user's computer to communicate directly with Pharmatrak's web server. When the user's computer requested the clear GIF, Pharmatrak's web servers responded by either placing or accessing a "persistent cookie" on the user's computer. On a user's first visit to a webpage monitored by NETcompare, Pharmatrak's servers would plant a cookie on the user's computer. If the user had already visited a NETcompare webpage, then Pharmatrak's servers would access the information on the existing cookie.

A cookie is a piece of information sent by a web server to a web browser that the browser software is expected to save and to send back whenever the browser makes additional requests of the server (such as when the user visits additional webpages at the same or related sites). A persistent cookie is one that does not expire at the end of an online session. Cookies are widely used on the internet by reputable websites to promote convenience and customization. Cookies often store user preferences, login and registration information, or information related to an online "shopping cart." Cookies may also contain unique identifiers that allow a website to differentiate among users.

Each Pharmatrak cookie contained a unique alphanumeric identifier that allowed Pharmatrak to track a user as she navigated through a client's site and to identify a repeat user each time she visited clients' sites. If a person visited www.pfizer.com in June 2000 and www.pharmacia.com in July 2000, for example, then the persistent cookie on her computer would indicate to Pharmatrak that the same computer had been used to visit both sites.[5] As NETcompare tracked a user through a website, it used JavaScript and a JavaApplet to record information such as the URLs the user visited. This data was recorded on the access logs of Pharmatrak's web servers.

Pharmatrak sent monthly reports to its clients juxtaposing the data collected by NETcompare about all pharmaceutical clients. These reports covered topics such as the most heavily used parts of a particular site; which site was receiving the most hits in particular areas such as investor or media relations; and the most important links to a site.

The monthly reports did not contain any personally identifiable information about users. The only information provided by Pharmatrak to clients about their users and traffic was contained in

[5] Pharmatrak's cookies expired after ninety days.

the reports (and executive summaries thereof). Slides from a Pharmatrak marketing presentation did say the company would break data out into categories and provide "user profiles." In practice, the aggregate demographic information in the reports was limited to the percentages of users from different countries; the percentages of users with different domain extensions (i.e., the percentages of users originating from for-profit, government, academic, or other not-for-profit organizations); and the percentages of first-time versus repeat users. An example of a NETcompare "user profile" is: "The average Novartis visitor is a first-time visitor from the U.S., visiting from a .com domain."

While it was marketing NETcompare to prospective pharmaceutical clients, Pharmatrak repeatedly told them that NETcompare did not collect personally identifiable information. It said its technology could not collect personal information, and specifically provided that the information it gathered could not be used to identify particular users by name. In their affidavits and depositions, executives of Pharmatrak clients consistently said that they believed NETcompare did not collect personal information, and that they did not learn otherwise until the onset of litigation. Some, if not all, pharmaceutical clients explicitly conditioned their purchase of NETcompare on Pharmatrak's guarantees that it would not collect users' personal information. For example, Pharmacia's April 2000 contract with Pharmatrak provided that NETcompare would not collect personally identifiable information from users. Michael Sonnenreich, Chief Executive Officer of Pharmatrak, stated unequivocally at his deposition that none of his company's clients consented to the collection of personally identifiable information.

Pharmatrak nevertheless collected some personal information on a small number of users. Pharmatrak distributed approximately 18.7 million persistent cookies through NETcompare. The number of unique cookies provides a rough estimate of the number of users Pharmatrak monitored.[9] Plaintiffs' expert was able to develop individual profiles for just 232 users.

The following personal information was found on Pharmatrak servers: names, addresses, telephone numbers, email addresses, dates of birth, genders, insurance statuses, education levels, occupations, medical conditions, medications, and reasons for visiting the particular website. Pharmatrak also occasionally recorded the subject, sender, and date of the web-based email message a user was reading immediately prior to visiting the website of a Pharmatrak client. Most of the individual profiles assembled by plaintiffs' expert contain some but not all of this information.

The personal information in 197 of the 232 user profiles was recorded due to an interaction between NETcompare and computer code written by one pharmaceutical client, Pharmacia, for one of its webpages. Starting on or before August 18, 2000 and ending sometime between December 2, 2000 and February 6, 2001, the client Pharmacia used the "get" method to transmit information from a rebate form on its Detrol website; the webpage was subsequently modified to use the "post" method of transmission. This was the source of the personal information collected by Pharmatrak from users of the Detrol website.

[9] Different users might have the same cookie (if, say, family members shared a computer and browser) or one user might have multiple cookies (if, for example, he used separate work and home computers to visit sites employing NETcompare, or if he revisited a NETcompare site after his first cookie expired).

Web servers use two methods to transmit information entered into online forms: the get method and the post method. The get method is generally used for short forms such as the "Search" box at Yahoo! and other online search engines. The post method is normally used for longer forms and forms soliciting private information. When a server uses the get method, the information entered into the online form becomes appended to the next URL. For example, if a user enters "respiratory problems" into the query box at a search engine, and the search engine transmits this information using the get method, then the words "respiratory" and "problems" will be appended to the query string at the end of the URL of the webpage showing the search results. By contrast, if a website transmits information via the post method, then that information does not appear in the URL. Since NETcompare was designed to record the full URLs of the webpages a user viewed immediately before and during a visit to a client's site, Pharmatrak recorded personal information transmitted using the get method.

There is no evidence Pharmatrak instructed its clients not to use the get method. The detailed installation instructions Pharmatrak provided to pharmaceutical clients ignore entirely the issue of the different transmission methods.

In addition to the problem at the Detrol website, there was also another instance in which a pharmaceutical client used the get method to transmit personal information entered into an online form. The other personal information on Pharmatrak's servers was recorded as a result of software errors. These errors were a bug in a popular email program (reported in May 2001 and subsequently fixed) and an aberrant web browser.

II.

On June 28, 2001, plaintiffs filed an amended consolidated class action complaint[13] against Pharmatrak; its parent company, Glocal Communications, Ltd.; and five pharmaceutical companies: American Home Products Corp., Glaxo Wellcome, Inc., Pfizer, Inc., Pharmacia Corp., and SmithKline Beecham Corp. Plaintiffs alleged nine counts including violation of Title I of the ECPA, 18 U.S.C. § 2510 et seq.; violation of Title II of the ECPA, 18 U.S.C. 2701 et seq.; violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; violation of Mass. Gen. Laws ch. 272, § 99; violation of Mass. Gen. Laws ch. 93A; invasion of privacy; trespass to chattels and conversion; and unjust enrichment….

The plaintiffs employed computer scientist C. Matthew Curtin and his company, Interhack, to analyze Pharmatrak's servers between December 17, 2001 and January 18, 2002. In about an hour, Curtin wrote three custom computer programs, including "getneedle.pl," to extract and organize personal information on Pharmatrak's web server access logs, which he "colloquially termed 'haystacks.'" Curtin then cross-referenced the information he extracted with other sources such as internet telephone books….

[13] Originally, eight lawsuits were filed in the District of Massachusetts and the Southern District of New York. The two lawsuits in the District of Massachusetts were filed on August 18, 2000. On April 18, 2001, the Judicial Panel on Multi-District Litigation issued an order transferring the six New York cases to the District of Massachusetts. The purported class, which has never been certified, consists of all persons who visited one of the defendants' websites "and who, as a result thereof, have had Pharmatrak 'cookies' placed upon their computers and have had information about them gathered by Pharmatrak."

III….

B. Elements of the ECPA Cause of Action

ECPA amended the Federal Wiretap Act by extending to data and electronic transmissions the same protection already afforded to oral and wire communications. The paramount objective of the Wiretap Act is to protect effectively the privacy of communications.

The post-ECPA Wiretap Act provides a private right of action against one who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." The Wiretap Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." Thus, plaintiffs must show five elements to make their claim under Title I of the ECPA: that a defendant (1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication (5) using a device. This showing is subject to certain statutory exceptions, such as consent.

In its trial and appellate court briefs, Pharmatrak sought summary judgment on only one element of § 2511(1)(a), interception, as well as on the statutory consent exception. We address these issues below. Pharmatrak has not contested whether it used a device or obtained the contents of an electronic communication. This is appropriate. The ECPA adopts a "broad, functional" definition of an electronic communication. This definition includes "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric, or photooptical system that affects interstate or foreign commerce," with certain exceptions unrelated to this case. Transmissions of completed online forms, such as the one at Pharmacia's Detrol website, to the pharmaceutical defendants constitute electronic communications.

The ECPA also says that "'contents,' when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." This definition encompasses personally identifiable information such as a party's name, date of birth, and medical condition. Finally, it is clear that Pharmatrak relied on devices such as its web servers to capture information from users.

C. Consent Exception

There is a pertinent statutory exception to § 2511(1)(a) "where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act...." Plaintiffs, of course, bear the burden of establishing a violation of the ECPA. Our case law is unclear as to who has the burden of showing the statutory exception for consent….We think, at least for the consent exception under the ECPA in civil cases, that it makes more sense to place the burden of showing consent on the party seeking the benefit of the exception, and so hold. That party is more likely to have evidence pertinent to the issue of consent. Plaintiffs do not allege that

Pharmatrak acted with a criminal or tortious purpose. Therefore, the question under the exception is limited to whether the pharmaceutical defendants gave consent to the interception. Because the district court disposed of the case on the grounds that Pharmatrak's conduct fell within the consent exception, we start there.

The district court adopted Pharmatrak's argument that the only relevant inquiry is whether the pharmaceutical companies consented to use Pharmatrak's NETcompare service, regardless of how the service eventually operated. In doing so, the district court did not apply this circuit's general standards for consent under the Wiretap Act and the ECPA set forth in *Griggs-Ryan*, 904 F.2d 112. It also misread two district court opinions on which it purported to rely.

This court addressed the issue of consent under the Wiretap Act in *Griggs-Ryan*. A party may consent to the interception of only part of a communication or to the interception of only a subset of its communications. "Thus, 'a reviewing court must inquire into the dimensions of the consent and then ascertain whether the interception exceeded those boundaries.'" Consent may be explicit or implied, but it must be actual consent rather than constructive consent. Pharmatrak argues that it had implied consent from the pharmaceutical companies.

Consent "should not casually be inferred." "Without actual notice, consent can only be implied when the surrounding circumstances convincingly show that the party knew about and consented to the interception."

The district court made an error of law, urged on it by Pharmatrak, as to what constitutes consent. It did not apply the standards of this circuit. Moreover, *DoubleClick* and *Avenue A* do not set up a rule, contrary to the district court's reading of them, that a consent to interception can be inferred from the mere purchase of a service, regardless of circumstances. If these cases did so hold, they would be contrary to the rule of this circuit established in *Griggs-Ryan*. *DoubleClick* and *Avenue A*, rather, were concerned with situations in which the defendant companies' clients purchased their services for the precise purpose of creating individual user profiles in order to target those users for particular advertisements. This very purpose was announced by DoubleClick and Avenue A publicly, as well as being self-evident. These decisions found it would be unreasonable to infer that the clients had not consented merely because they might not understand precisely how the user demographics were collected. The facts in our case are the mirror image of those in *DoubleClick* and *Avenue A*: the pharmaceutical clients insisted there be no collection of personal data and the circumstances permit no reasonable inference that they did consent.

On the undisputed facts, the client pharmaceutical companies did not give the requisite consent. The pharmaceutical clients sought and received assurances from Pharmatrak that its NETcompare service did not and could not collect personally identifiable information. Far from consenting to the collection of personally identifiable information, the pharmaceutical clients explicitly conditioned their purchase of NETcompare on the fact that it would not collect such information.

The interpretation urged by Pharmatrak would, we think, lead to results inconsistent with the statutory intent. It would undercut efforts by one party to a contract to require that the privacy

interests of those who electronically communicate with it be protected by the other party to the contract. It also would lead to irrational results. Suppose Pharmatrak, for example, had intentionally designed its software, contrary to its representations and its clients' expectations, to redirect all possible personal information to Pharmatrak servers, which collected and mined the data. Under the district court's approach, Pharmatrak would nevertheless be insulated against liability under the ECPA on the theory that the pharmaceutical companies had "consented" by simply buying Pharmatrak's product. Or suppose an internet service provider received a parent's consent solely to monitor a child's internet usage for attempts to access sexually explicit sites—but the ISP installed code that monitored, recorded and cataloged all internet usage by parent and child alike. Under the theory we have rejected, the ISP would not be liable under the ECPA.

Nor did the users consent. On the undisputed facts, it is clear that the internet user did not consent to Pharmatrak's accessing his or her communication with the pharmaceutical companies. The pharmaceutical companies' websites gave no indication that use meant consent to collection of personal information by a third party. Rather, Pharmatrak's involvement was meant to be invisible to the user, and it was. Deficient notice will almost always defeat a claim of implied consent. Pharmatrak makes a frivolous argument that the internet users visiting client Pharmacia's webpage for rebates on Detrol thereby consented to Pharmatrak's intercepting their personal information. On that theory, every online communication would provide consent to interception by a third party.

D. Interception Requirement

The parties briefed to the district court the question of whether Pharmatrak had "intercepted" electronic communications. If this question could be resolved in Pharmatrak's favor, that would provide a ground for affirmance of the summary judgment. It cannot be answered in favor of Pharmatrak.

The ECPA prohibits only "interceptions" of electronic communications. "Intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."

Before enactment of the ECPA, some courts had narrowed the Wiretap Act's definition of interception to include only acquisitions of a communication contemporaneous with transmission. There was a resulting debate about whether the ECPA should be similarly restricted….Other circuits have invoked the contemporaneous, or "real-time," requirement to exclude acquisitions apparently made a substantial amount of time after material was put into electronic storage. These circuits have distinguished between materials acquired in transit, which are interceptions, and those acquired from storage, which purportedly are not.

We share the concern of the Ninth and Eleventh Circuits about the judicial interpretation of a statute written prior to the widespread usage of the internet and the World Wide Web in a case involving purported interceptions of online communications. In particular, the storage-transit dichotomy adopted by earlier courts may be less than apt to address current problems. As one court recently observed, "[T]echnology has, to some extent, overtaken language. Traveling the

internet, electronic communications are often—perhaps constantly—both 'in transit' and 'in storage' simultaneously, a linguistic but not a technological paradox."

The facts here do not require us to enter the debate over the existence of a real-time requirement. The acquisition by Pharmatrak was contemporaneous with the transmission by the internet users to the pharmaceutical companies. Both Curtin, the plaintiffs' expert, and Wes Sonnenreich, Pharmatrak's former CTO, observed that users communicated simultaneously with the pharmaceutical client's web server and with Pharmatrak's web server. After the user's personal information was transmitted using the get method, both the pharmaceutical client's server and Pharmatrak's server contributed content for the succeeding webpage; as both Curtin and Wes Sonnenreich acknowledged, Pharmatrak's content (the clear GIF that enabled the interception) sometimes arrived before the content delivered by the pharmaceutical clients.

Even those courts that narrowly read "interception" would find that Pharmatrak's acquisition was an interception. For example, *Steiger* observes:

> [U]nder the narrow reading of the Wiretap Act we adopt ..., very few seizures of electronic communications from computers will constitute 'interceptions.' ... 'Therefore, unless some type of automatic routing software is used (for example, a duplicate of all of an employee's messages are automatically sent to the employee's boss), interception of E-mail within the prohibition of [the Wiretap Act] is virtually impossible.'

NETcompare was effectively an automatic routing program. It was code that automatically duplicated part of the communication between a user and a pharmaceutical client and sent this information to a third party (Pharmatrak).

Pharmatrak argues that there was no interception because "there were always two separate communications: one between the Web user and the Pharmaceutical Client, and the other between the Web user and Pharmatrak." This argument fails for two reasons. First, as a matter of law, even the circuits adopting a narrow reading of the Wiretap Act merely require that the acquisition occur at the same time as the transmission; they do not require that the acquisition somehow constitute the same communication as the transmission. Second, Pharmatrak acquired the same URL query string (sometimes containing personal information) exchanged as part of the communication between the pharmaceutical client and the user. Separate, but simultaneous and identical, communications satisfy even the strictest real-time requirement.

E. Intent Requirement

At oral argument this court questioned the parties about whether the "intent" requirement under § 2511(a)(1) had been met.

We remand this issue because it was not squarely addressed by both parties before the district court. When Pharmatrak moved for summary judgment, it did not do so on the grounds that the statutory requirement of intent was unmet. At most, it raised the issue in passing at the hearing on the cross-motions for summary judgment.

Plaintiffs, in their motion for summary judgment, did raise the issue and argued that any interception was intentional; but the district court neither granted the motion nor addressed the issue. In its opposition to plaintiffs' motion, Pharmatrak relied on its own motion for summary judgment, and so did not address intent. The issue has not been briefed to us.

While it is true that we can affirm the grant of summary judgment on any ground presented by the record, we will usually do so only when the issue has been fairly presented to the trial court. Here it was not, and we are reluctant to determine ourselves whether there was adequate opportunity for discovery on this issue and whether there are material facts in dispute, and to resolve an issue without briefing.

Still, we wish to avoid uncertainty about the legal standard for intent under the ECPA on remand, and so we address that point. Congress amended 18 U.S.C. § 2511 in 1986 to change the state of mind requirement from "willful" to "intentional". Since "intentional" itself may have different glosses put on it, we refer to the legislative history, which states:

> As used in the Electronic Communications Privacy Act, the term "intentional" is narrower than the dictionary definition of "intentional." "Intentional" means more than that one voluntarily engaged in conduct or caused a result. Such conduct or the causing of the result must have been the person's conscious objective. An "intentional" state of mind means that one's state of mind is intentional as to one's conduct or the result of one's conduct if such conduct or result is one's conscious objective. The intentional state of mind is applicable only to conduct and results. Since one has no control over the existence of circumstances, one cannot "intend" them.

S.Rep. No. 99-541, at 23 (1986). Congress made clear that the purpose of the amendment was to underscore that inadvertent interceptions are not a basis for criminal or civil liability under the ECPA. Id. An act is not intentional if it is the product of inadvertence or mistake. There is also authority suggesting that liability for intentionally engaging in prohibited conduct does not turn on an assessment of the merit of a party's motive. That is not to say motive is entirely irrelevant in assessing intent. An interception may be more likely to be intentional when it serves a party's self-interest to engage in such conduct.

F. Conclusion

We reverse and remand for further proceedings consistent with this opinion.

Eric Goldman, *Where's the Beef? Dissecting Spam's Purported Harms*, 22 J. MARSHALL J. COMPUTER & INFO. L. 13 (2003).

I. INTRODUCTION

After many failed attempts over the past six years, Congress finally enacted a law regulating unsolicited commercial e-mails, the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the "CAN-SPAM Act" or "CAN-SPAM"). CAN-SPAM follows significant state-based efforts to regulate spam; from 1997 to 2003, nearly three quarters of the states adopted some spam regulation, most of which are now preempted by CAN-SPAM.

CAN-SPAM, like the state laws preceding it, takes a multi-faceted approach to regulating spam. Among other provisions, CAN-SPAM contains provisions that regulate the e-mail content, restrict specific notorious spammer practices, give spam recipients the ability to opt-out, and attack the spammer's funding by creating advertiser liability.

The diversity of regulatory approaches inherent in CAN-SPAM (and, before that, the superseded state statutes) prompts a fundamental question: exactly what harms are caused by spam that these regulations attempt to redress? There is no consensus answer to this question. Just about everyone seems to agree that spam is a problem that needs to be addressed, but no one seems to agree on why. Without clearly understanding the targeted harms, policy-makers cannot craft regulations designed to fix them.

This Essay examines the purported harms caused by spam in an effort to isolate bona fide areas needing legislative intervention. However, few such needs exist. Instead, most purported harms are illusory, already adequately addressed by existing laws or best left to market solutions. This analysis thus undercuts many of the purported justifications for regulating spam.

II. DEFINING THE HARMS OF SPAM

A. Defining Spam

Any attempt to intelligently discuss spam is immediately hampered by the word's imprecision. Simply put, the term "spam" lacks a single well-accepted definition. Usually "spam" refers to some form of unwanted e-mail, although some users generalize the term to describe all forms of unwanted advertising, both in e-mail and other media. CAN-SPAM defines "commercial electronic mail message" as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service." Building on this definition, this Essay refers to "spam" as unsolicited "commercial electronic mail messages." However, this definition is both under- and over-inclusive because the definition includes e-mails recipients want and does not include all e-mails not wanted by recipients, and thus it may not track recipient expectations.

B. Spam is Annoying

1. Distinguishing Wanted and Unwanted Content

Many e-mail recipients castigate spam as annoying, but the reasons why are less clear. Some annoyance is attributable to the objectionable content in spam, a point addressed infra in subsection II(D). Otherwise, the annoyance is based (among other factors) on the unsolicited, high-volume, time-consuming or unpreventable nature of spam.

I believe these concerns all derive from the same source: spam is unwanted. A simple example may illustrate this. Assume Jane is ready to purchase a Canon PowerShot S400 digital camera. An unsolicited e-mail arrives in Jane's in-box from a trustworthy retailer that she has never transacted with. The retailer offers to sell her the camera for $100 less than any other retailer. Is this spam?

Some recipients would say "yes" because the e-mail is unsolicited or otherwise invades their privacy. However, most e-mail recipients would consider this e-mail valuable instead of annoying, in which case they would want this e-mail because it will save them time and money. Perhaps this example gives us an important insight on the nature of spam. E-mail recipients want e-mail that saves money, saves time, educates on matters of interest, or is otherwise relevant and helpful. Thus, many e-mail recipients gladly would receive unsolicited e-mails that meet those specifications. In contrast, e-mail recipients are annoyed to receive a high volume of irrelevant and unhelpful e-mails.

Unfortunately, frequently spam is irrelevant and unhelpful to recipients because it is relatively untargeted. Like any other marketers, spam advertisers will pay for targeted e-mail lists that are more likely to yield higher results. However, the negligible marginal cost of sending spam lowers the optimal level of targeting for spammers. Thus, spammers can profitably use low-yield and untargeted practices such as e-mail harvesting and dictionary attacks.

Even though spammers can profitably send very-low relevance e-mails to lots of recipients, not all spam is bad. Inevitably, some recipients will find a particular spam e-mail helpful and relevant. More specifically, recipients' perceptions about each spam's relevance usually sort into a bell curve: some will find the e-mail completely irrelevant, some will find the e-mail very relevant, and others will find the e-mail somewhat relevant.

Some empirical data supports this analysis. Several recent surveys show that seven to eight percent of those surveyed have purchased a product or service in response to spam and approximately thirty percent of those surveyed have responded to spam to get more information about the advertised product or service. While not high percentages, the statistics seemingly contradict spam's abysmal reputation. For recipients who responded to spam (plus those who were educated but did not respond), the spam was relevant. For those who purchased in response to a particular spam, that e-mail helped the consumer find a desired product or service at an acceptable price.

We should not trivialize these consequences. Spam plays an important role in the marketplace of ideas, perhaps filling gaps left by other media, and can contribute to efficiently functioning economic markets. In some cases, spam creates transaction opportunities that otherwise would not occur due to prohibitive search costs or lack of consumer awareness about products available to solve their needs.

Of course, these conclusions do not change the fact that most spam is unwanted by most recipients. However, it is unclear why individuals seem less tolerant of irrelevant spam than irrelevant ads in other media. Consumers routinely tolerate irrelevant ads in other media with less annoyance than they feel towards spam.

Let us consider ad relevancy in a few media, starting with billboards. Billboard ads target viewers only by geography (if that), so they are fairly low-relevancy advertising tools, meaning that most billboard ads will be irrelevant to most viewers.

The broadcast and newspaper media use differentiated content to segment consumers. Thus, a TV show will appeal to a certain demographic, and newspapers divide their content into topical sections (e.g. sports, business, metro) that are read by only some readers. This segmentation means that ads can be targeted to consumers attracted by the surrounding content. Nevertheless, even the most targeted content will appeal to multiple demographics, so the associated ads will be less relevant to non-majority audience segments.

In these other media like billboards, broadcasting and newspapers, consumers do not vociferously demand regulation to minimize the irrelevancy of ads delivered through them. Why do consumers feel differently about spam?

2. Sorting Spam Wastes Time

Perhaps recipients penalize spam because it takes time to sort irrelevant spam from wanted e-mails. Sorting also creates the risk of Type I and Type II errors (i.e., legitimate e-mail gets tossed or blocked as spam, and objectionable spam gets through the sorting).

But once again, spam is not different from other media. Every medium that contains ads requires consumers to sort ads from content and wanted ads from unwanted ads. For example, sorting postal mail requires the recipient to evaluate the envelope's exterior and, in some cases, open and review the contents. Broadcast ads are even more difficult to sort, because ads are interspersed with content and the viewer cannot reorder or skip the ads.

So while spam does require sorting time, recipients can manually sort e-mail relatively efficiently by reviewing subject lines, and many recipients develop good skills doing so. Spam can also be automatically blocked without any manual sorting using e-mail filters. As a result, the amount of time "wasted" on the e-mail sorting process may very well be less than the time wasted in other media.

All media containing ads demand sorting time and create some risk of erroneous sorting, and no regulatory scheme—other than banning a medium altogether—can eliminate that. Instead, time lost to sorting is unavoidable in a media-based society, and spam is just one of many manifestations of that phenomenon. Thus, the explanation for recipients' antipathy towards spam must lie elsewhere.

3. Spam Causes Recipients to Lose Control of Their In-Boxes

Evidence suggests that many recipients are bothered by their inability to stop spam and feel that spam is a loss of privacy. This suggests that recipient frustration with spam may be the result of a feeling that recipients have lost control over their in-boxes.

However, once again this problem arises with other media. Recipients cannot stop spam except by eliminating their e-mail account altogether, but consumers of other media are similarly powerless to change what ads are delivered in that medium except by discontinuing use of that medium. For example, a newspaper or magazine reader cannot control what ads are published; the reader's only choices are to ignore unwanted ads or stop reading the publication altogether. This argument holds true for broadcast media, billboards, and junk mail as well.

Perhaps e-mail can be distinguished from other media because it delivers more important personal content to recipients than other media. Recipients seem to develop a special and personal relationship with their in-box, and this explanation might offer an insight about why telemarketing is so reviled. But this explanation is not totally satisfactory because it does not explain the seeming dichotomy between the outrage over spam and comparative tolerance of junk mail.

A more satisfying explanation can be found by considering the relative adoption curves of spam and other media. We have had many years to develop ways to cope with ads in other media, but we are still developing ways to cope with e-mail ads. It seems likely that users will improve their ability to manage e-mail with more experience, at which point user frustration should decrease. Meanwhile, new generations who grow up using e-mail should be more tolerant of spam because they will develop coping strategies for spam (and media inputs generally) from an early age.

Thus, current annoyance with spam could merely reflect that user experience with e-mail is evolving. Robust e-mail management tools also should reduce annoyance, and the current annoyance may also reflect that those tools are not yet adequately deployed.

4. Conclusion on Annoyance

Unwanted e-mails are annoying, but minor annoyances are a fact of life, and no law can eliminate them—from e-mail or otherwise. E-mail recipients' annoyance at spam appears to be an overreaction when compared to their reactions to other forms of annoying ads. Meanwhile, regulation of spam creates significant risk that some relevant e-mails will be blocked from recipients who want them. It is troubling to regulate content to protect the majority from minor annoyances if the consequence is preventing minority interests from exchanging relevant content.

C. Spammers Impose Costs on Third Parties

As it moves from sender to recipient, spam generates bandwidth and server processing costs for the spammer's IAP, the recipient and the recipient's IAP. Depending on a spammer's practices, they can also impose some costs on unsuspecting third parties, such as server operators with open mail relays and or whose domains are forged. We consider each cost in turn.

1. The Spammer's IAP

The spammer and its IAP have contractual privity, and the IAP can technologically constrain the spammer's activities (i.e. capping the quantity of e-mails sent). As a result, a spammer's IAP has the capacity to charge spammers for any spam-related costs, and there are no obvious market failures that require regulatory protection for the spammer's IAP.

2. Recipients and Their IAPs

It is frequently claimed that recipients pay to receive spam, and sometimes spam is likened to junk mail sent with postage due. With respect to individuals with a consumer IAP account, this claim is no longer accurate. It was true prior to the mid-1990s, when many IAPs charged customers a time-based fee for Internet connectivity. Because each e-mail took some time to download, recipients paid a small fee for each e-mail they received. Today, consumer IAPs almost universally charge flat-rate pricing for unlimited usage, so consumer recipients do not pay for each e-mail received.

However, recipient IAPs bear some bandwidth and server processing costs for each e-mail they process, plus preventative costs (like filtering) and remediation costs (like blocking or database repair) associated with pernicious e-mail. Unlike the spammer's IAP, the recipient's IAP has no contractual privity or technological relationship with the spammer. And where corporations provide Internet connectivity to their employees, they incur these costs as a recipient directly. As a result, recipient IAPs and corporations may benefit from legal systems that allow them to pass those costs back to spammers or avoid the costs altogether.

Until recently, common law trespass to chattels was an important legal mechanism to accomplish that objective. However, in *Intel Corp. v. Hamidi*, the California Supreme Court recently scaled the doctrine back, rejecting trespass to chattels when a low-volume spammer's e-mails did not threaten to impair (or actually impair) the functioning of Intel's systems. It remains unclear how subsequent courts will interpret *Intel*, but in all likelihood some future spammers will avoid liability for trespass to chattels.

Irrespective of trespass to chattels, corporations and recipient IAPs can use, and have successfully used, the Computer Fraud and Abuse Act ("CFAA") to combat spam. CAN-SPAM supplements the CFAA (and whatever is left of common law trespass to chattels) by providing recipient IAPs a direct cause of action when the IAP is "adversely affected" by a spammer who fails to comply with selected other provisions of CAN-SPAM. Depending on how broadly courts interpret the words "adversely affected," this provision may moot Hamidi's common law analysis by providing a statutory cause of action. At minimum, CAN-SPAM expedites recipient IAP causes of action by providing statutory damages and attorneys' fees and by providing another basis (in addition to the CFAA) for federal court jurisdiction. As a result, CAN-SPAM should help recipient IAPs control some of the e-mail processing costs that are externalized to them.

In addition to bandwidth, server, preventative and maintenance costs, some companies have sought legal recognition for the time employees waste on spam. Indeed, analysts claim that this lost time creates enormous costs. However, as discussed in Section II supra, time spent sorting or reading spam is not necessarily wasted, nor is it unique compared to the many other ways that

employees waste time (e.g. personal e-mail, junk mail and personal telephone calls). Therefore, lost productivity due to spam is a poor policy basis for regulating spam.

3. Open Mail Relays

Spammers can offload costs to third party computers who have open mail relays, which can cause those server operators to incur some costs like any other recipient IAP. Of course, operators wishing to avoid those costs can simply close their mail relays, and interestingly these operators are often considered part of the problem, not victims. Thus, forcing them to internalize the spam-created costs (rather than pushing those costs to a spammer) may motivate them to close the relays.

4. Targets of Forged Headers

Spammers also can offload costs to third parties using forged headers. A forged header occurs when a spammer manipulates an e-mail to make it look like the spam originated from X.com when it is really being sent from Y.com. The X.com domain name operator (or its IAP) incurs costs when undeliverable messages and recipient complaints are directed to the operator.

The operator of a forged domain name lacks any contractual or technological way to prevent this activity, so regulatory protection is appropriate. Indeed, thirty states prohibited forged headers, and these state laws may not be preempted by CAN-SPAM. Meanwhile, CAN-SPAM criminalizes forged headers and potentially sets up a private cause of action for some victims ("providers of Internet access services" who are "adversely affected"). The robustness of this private cause of action remains to be seen, but this CAN-SPAM provision, plus any coverage under non-preempted state laws and other existing doctrines like trademark law and the CFAA, should provide substantial protection to the victims of forged headers.

5. Conclusion on Costs

Far too much rhetoric is directed to the costs borne by individual spam recipients. These individuals no longer bear a financial cost to receive spam, and any "costs" associated with the consumption of their attention makes unsupportable assumptions about the e-mail's relevancy to the recipient. Similarly, although sending IAPs may find it desirable to obtain regulatory protection against spam, they can control their financial exposure to spammers' behavior through pricing and technology.

Focusing on the costs borne by individual recipients and sending IAPs detracts from the parties who incur uncontrollable costs from spam, such as recipient IAPs, operators of open mail relays and victims of forged headers. CAN-SPAM provides some useful legal tools to protect these parties, although those tools may be incomplete. A crisper understanding of the real costs borne by these parties would have likely produced a more thoughtful legal solution.

D. Spam Contains or Promotes Objectionable Content

Many spam recipients complain about objectionable content of spam, especially pornographic spam. Due to deep feelings towards pornographic spam, Congress specifically targeted it in CAN-SPAM by requiring warning labels. But to understand the harms pornographic spam causes, it is useful to consider adults and minors separately.

For adults, pornographic spam is no different from any other form of unwanted content discussed in Section II(B) supra. Nevertheless, Congress has tried to help adults avoid unwanted pornographic spam by requiring special labeling of pornographic spam in the subject line. When implemented, this requirement can help recipients who automatically filter e-mail using the appropriate words because the spam will automatically be routed outside the recipient's ordinary view. Until spammers regularly comply with this law, however, filtering will not be helpful.

The mandatory labeling law may be even less helpful to recipients who manually sort e-mail. These recipients may still see objectionable content if the subject line contains objectionable terms or the recipient's e-mail software "previews" a message and the previewed content is objectionable.

So how can regulatory intervention help recipients avoid objectionable e-mails? With widely varying perceptions of what constitutes objectionable content, regulating objectionable ads is no more feasible than regulating irrelevant ads. Thus, the only "solution" may be for recipients to manage their exposures themselves, either through technological measures or by looking elsewhere when something offends.

Putting the burden on recipients to avoid pornographic spam is less satisfactory when recipients are minors. In that case, society may be harmed when minors view this inappropriate material.

However, minors' exposure to pornographic spam is a microcosm of a much greater problem: minors with e-mail accounts. This is a major social development because historically minors had few communication media that readily bypassed parental oversight. Today, minors can use e-mail, instant messenger, and cell phones to communicate with third parties without any parental oversight and knowledge. With this additional autonomy, minors can get into inappropriate and potentially very dangerous situations, such as interactions with sexual predators.

Because of these risks, some parents restrict minors' access to the Internet altogether, and other parents permit only supervised Internet use. The former prevents any risk of exposure to pornographic spam, and the latter approach gives parents the ability to pre-screen pornographic spam or counsel the minor when seeing such spam.

Otherwise, parents who let minors have unsupervised e-mail use make a huge decision, and it is not made lightly. Because these parents accept the risk that their children will engage in dangerous online behavior, the problem of pornographic spam seems almost trivial by comparison. If the parents trust their children enough to give them that autonomy, perhaps we should infer that the parents deem their children responsible enough to cope with pornographic spam.

Regulation cannot easily solve these problems. Efforts to specifically ban pornographic spam are likely unconstitutional and do not affect e-mails from foreign jurisdictions. Lesser efforts, like mandatory labeling, have low efficacy. Ultimately, there can be no substitute for parental involvement in their children's use of e-mail.

III. CONCLUSION

Society is still evolving ways to cope with media saturation. Spam contributes to this problem, but so do other media. Yet, many recipients hate spam more than other ads. As explored by this Essay, this dichotomous attitude is hard to explain. Nevertheless, the anger has caused anti-spam rhetoric to reach hyperbolic levels. But, while many spam opponents decry spam as a system breakdown, the breakdown has been more political than technological. Most state-based attempts to regulate spam, a product of political grandstanding or legislator rage instead of rational policy-making, were ineffectual, reflecting their weak policy underpinnings. Early feedback on CAN-SPAM suggests the federal law will not be any more effective.

Even if CAN-SPAM beneficially affects the flow of unwanted e-mails, any legislative solution seems inherently empty. Without legislative intervention, society will find ways to cope with spam, just as we have with other media. Meanwhile, entrepreneurs will continue to develop better tools to sort wanted and unwanted communications. Thus, more patience with the spam "problem" might have facilitated the development of superior results organically.

15 U.S.C. §7701-7713 (the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003" or the "CAN-SPAM Act of 2003").

15 U.S.C. § 7701: CONGRESSIONAL FINDINGS AND POLICY. (CAN-SPAM Section 2)

(a) FINDINGS.—The Congress finds the following:
(1) Electronic mail has become an extremely important and popular means of communication, relied on by millions of Americans on a daily basis for personal and commercial purposes. Its low cost and global reach make it extremely convenient and efficient, and offer unique opportunities for the development and growth of frictionless commerce.
(2) The convenience and efficiency of electronic mail are threatened by the extremely rapid growth in the volume of unsolicited commercial electronic mail. Unsolicited commercial electronic mail is currently estimated to account for over half of all electronic mail traffic, up from an estimated 7 percent in 2001, and the volume continues to rise. Most of these messages are fraudulent or deceptive in one or more respects.
(3) The receipt of unsolicited commercial electronic mail may result in costs to recipients who cannot refuse to accept such mail and who incur costs for the storage of such mail, or for the time spent accessing, reviewing, and discarding such mail, or for both.
(4) The receipt of a large number of unwanted messages also decreases the convenience of electronic mail and creates a risk that wanted electronic mail messages, both commercial and noncommercial, will be lost, overlooked, or discarded amidst the larger volume of unwanted messages, thus reducing the reliability and usefulness of electronic mail to the recipient.
(5) Some commercial electronic mail contains material that many recipients may consider vulgar or pornographic in nature.
(6) The growth in unsolicited commercial electronic mail imposes significant monetary costs on providers of Internet access services, businesses, and educational and nonprofit institutions that carry and receive such mail, as there is a finite volume of mail that such providers, businesses, and institutions can handle without further investment in infrastructure.
(7) Many senders of unsolicited commercial electronic mail purposefully disguise the source of such mail.
(8) Many senders of unsolicited commercial electronic mail purposefully include misleading information in the messages' subject lines in order to induce the recipients to view the messages.
(9) While some senders of commercial electronic mail messages provide simple and reliable ways for recipients to reject (or "opt-out" of) receipt of commercial electronic mail from such senders in the future, other senders provide no such "opt-out" mechanism, or refuse to honor the requests of recipients not to receive electronic mail from such senders in the future, or both.
(10) Many senders of bulk unsolicited commercial electronic mail use computer programs to gather large numbers of electronic mail addresses on an automated basis from Internet websites or online services where users must post their addresses in order to make full use of the website or service.
(11) Many States have enacted legislation intended to regulate or reduce unsolicited commercial electronic mail, but these statutes impose different standards and requirements. As a result, they do not appear to have been successful in addressing the problems associated with unsolicited commercial electronic mail, in part because, since an electronic mail address does not specify a

geographic location, it can be extremely difficult for law-abiding businesses to know with which of these disparate statutes they are required to comply.
(12) The problems associated with the rapid growth and abuse of unsolicited commercial electronic mail cannot be solved by Federal legislation alone. The development and adoption of technological approaches and the pursuit of cooperative efforts with other countries will be necessary as well.

(b) CONGRESSIONAL DETERMINATION OF PUBLIC POLICY.—On the basis of the findings in subsection (a), the Congress determines that—
(1) there is a substantial government interest in regulation of commercial electronic mail on a nationwide basis;
(2) senders of commercial electronic mail should not mislead recipients as to the source or content of such mail; and
(3) recipients of commercial electronic mail have a right to decline to receive additional commercial electronic mail from the same source.

15 U.S.C. § 7702: DEFINITIONS. (CAN-SPAM Section 3)

In this Act:

(1) AFFIRMATIVE CONSENT.—The term "affirmative consent", when used with respect to a commercial electronic mail message, means that—

> (A) the recipient expressly consented to receive the message, either in response to a clear and conspicuous request for such consent or at the recipient's own initiative; and
> (B) if the message is from a party other than the party to which the recipient communicated such consent, the recipient was given clear and conspicuous notice at the time the consent was communicated that the recipient's electronic mail address could be transferred to such other party for the purpose of initiating commercial electronic mail messages.

(2) Commercial electronic mail message—

> (A) IN GENERAL.—The term "commercial electronic mail message" means any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose).
> (B) TRANSACTIONAL OR RELATIONSHIP MESSAGES.—The term "commercial electronic mail message" does not include a transactional or relationship message.
> (C) REGULATIONS REGARDING PRIMARY PURPOSE.—Not later than 12 months after the date of the enactment of this Act, the Commission shall issue regulations pursuant to section 13 defining the relevant criteria to facilitate the determination of the primary purpose of an electronic mail message.
> (D) REFERENCE TO COMPANY OR WEBSITE.—The inclusion of a reference to a commercial entity or a link to the website of a commercial entity in an electronic mail message does not, by itself, cause such message to be treated as a

commercial electronic mail message for purposes of this Act if the contents or circumstances of the message indicate a primary purpose other than commercial advertisement or promotion of a commercial product or service.

(3) COMMISSION.—The term “Commission” means the Federal Trade Commission.

(4) DOMAIN NAME.—The term “domain name” means any alphanumeric designation which is registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority as part of an electronic address on the Internet.

(5) ELECTRONIC MAIL ADDRESS.—The term “electronic mail address” means a destination, commonly expressed as a string of characters, consisting of a unique user name or mailbox (commonly referred to as the “local part”) and a reference to an Internet domain (commonly referred to as the “domain part”), whether or not displayed, to which an electronic mail message can be sent or delivered.

(6) ELECTRONIC MAIL MESSAGE.—The term “electronic mail message” means a message sent to a unique electronic mail address.

(7) FTC ACT.—The term “FTC Act” means the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

(8) HEADER INFORMATION.—The term “header information” means the source, destination, and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message.

(9) INITIATE.—The term “initiate”, when used with respect to a commercial electronic mail message, means to originate or transmit such message or to procure the origination or transmission of such message, but shall not include actions that constitute routine conveyance of such message. For purposes of this paragraph, more than one person may be considered to have initiated a message.

(10) INTERNET.—The term “Internet” has the meaning given that term in the Internet Tax Freedom Act (47 U.S.C. 151 nt).

(11) INTERNET ACCESS SERVICE.—The term “Internet access service” has the meaning given that term in section 231(e)(4) of the Communications Act of 1934 (47 U.S.C. 231(e)(4)).

(12) PROCURE.—The term “procure”, when used with respect to the initiation of a commercial electronic mail message, means intentionally to pay or provide other consideration to, or induce, another person to initiate such a message on one’s behalf.

(13) PROTECTED COMPUTER.—The term “protected computer” has the meaning given that term in section 1030(e)(2)(B) of title 18, United States Code.

(14) RECIPIENT.—The term “recipient”, when used with respect to a commercial electronic mail message, means an authorized user of the electronic mail address to which the message was sent or delivered. If a recipient of a commercial electronic mail message has one or more electronic mail addresses in addition to the address to which the message was sent or delivered, the recipient shall be treated as a separate recipient with respect to each such address. If an electronic mail address is reassigned to a new user, the new user shall not be treated as a recipient of any commercial electronic mail message sent or delivered to that address before it was reassigned.

(15) ROUTINE CONVEYANCE.—The term “routine conveyance” means the transmission, routing, relaying, handling, or storing, through an automatic technical process, of an electronic mail message for which another person has identified the recipients or provided the recipient addresses.

(16) SENDER.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term “sender”, when used with respect to a commercial electronic mail message, means a person who initiates such a message and whose product, service, or Internet web site is advertised or promoted by the message.

(B) SEPARATE LINES OF BUSINESS OR DIVISIONS.—If an entity operates through separate lines of business or divisions and holds itself out to the recipient throughout the message as that particular line of business or division rather than as the entity of which such line of business or division is a part, then the line of business or the division shall be treated as the sender of such message for purposes of this Act.

(17) Transactional or relationship message—

(A) IN GENERAL.—The term “transactional or relationship message” means an electronic mail message the primary purpose of which is—

(i) to facilitate, complete, or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender;

(ii) to provide warranty information, product recall information, or safety or security information with respect to a commercial product or service used or purchased by the recipient;

(iii) to provide—

(I) notification concerning a change in the terms or features of;

(II) notification of a change in the recipient’s standing or status with respect to; or

(III) at regular periodic intervals, account balance information or other type of account statement with respect to,

a subscription, membership, account, loan, or comparable ongoing commercial relationship involving the ongoing purchase or use by the recipient of products or services offered by the sender;

(iv) to provide information directly related to an employment relationship or related benefit plan in which the recipient is currently involved, participating, or enrolled; or
(v) to deliver goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender.

(B) MODIFICATION OF DEFINITION.—The Commission by regulation pursuant to section 13 may modify the definition in subparagraph (A) to expand or contract the categories of messages that are treated as transactional or relationship messages for purposes of this Act to the extent that such modification is necessary to accommodate changes in electronic mail technology or practices and accomplish the purposes of this Act.

15 U.S.C. § 7703: PROHIBITION AGAINST PREDATORY AND ABUSIVE COMMERCIAL E—MAIL. (CAN-SPAM Section 4)

(a) OFFENSE.—
(1) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by adding at the end the following new section:

"§ 1037. Fraud and related activity in connection with electronic mail
"(a) IN GENERAL.—Whoever, in or affecting interstate or foreign commerce, knowingly—
"(1) accesses a protected computer without authorization, and intentionally initiates the transmission of multiple commercial electronic mail messages from or through such computer,
"(2) uses a protected computer to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages,
"(3) materially falsifies header information in multiple commercial electronic mail messages and intentionally initiates the transmission of such messages,
"(4) registers, using information that materially falsifies the identity of the actual registrant, for five or more electronic mail accounts or online user accounts or two or more domain names, and intentionally initiates the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names, or
"(5) falsely represents oneself to be the registrant or the legitimate successor in interest to the registrant of 5 or more Internet Protocol addresses, and intentionally initiates the transmission of multiple commercial electronic mail messages from such addresses, or conspires to do so, shall be punished as provided in subsection (b).
"(b) PENALTIES.—The punishment for an offense under subsection (a) is—

"(1) a fine under this title, imprisonment for not more than 5 years, or both, if—

"(A) the offense is committed in furtherance of any felony under the laws of the United States or of any State; or

"(B) the defendant has previously been convicted under this section or section 1030, or under the law of any State for conduct involving the transmission of multiple commercial electronic mail messages or unauthorized access to a computer system;

"(2) a fine under this title, imprisonment for not more than 3 years, or both, if—

"(A) the offense is an offense under subsection (a)(1);

"(B) the offense is an offense under subsection (a)(4) and involved 20 or more falsified electronic mail or online user account registrations, or 10 or more falsified domain name registrations;

"(C) the volume of electronic mail messages transmitted in furtherance of the offense exceeded 2,500 during any 24-hour period, 25,000 during any 30- day period, or 250,000 during any 1-year period;

"(D) the offense caused loss to one or more persons aggregating $5,000 or more in value during any 1-year period;

"(E) as a result of the offense any individual committing the offense obtained anything of value aggregating $5,000 or more during any 1-year period; or

"(F) the offense was undertaken by the defendant in concert with three or more other persons with respect to whom the defendant occupied a position of organizer or leader; and

"(3) a fine under this title or imprisonment for not more than 1 year, or both, in any other case.

"(c) FORFEITURE.—

"(1) IN GENERAL.—The court, in imposing sentence on a person who is convicted of an offense under this section, shall order that the defendant forfeit to the United States—

"(A) any property, real or personal, constituting or traceable to gross proceeds obtained from such offense; and

"(B) any equipment, software, or other technology used or intended to be used to commit or to facilitate the commission of such offense.

"(2) PROCEDURES.—The procedures set forth in section 413 of the Controlled Substances Act (21 U.S.C. 853), other than subsection (d) of that section, and in Rule 32.2 of the Federal Rules of Criminal Procedure, shall apply to all stages of a criminal forfeiture proceeding under this section.

"(d) DEFINITIONS.—In this section:

"(1) LOSS.—The term 'loss' has the meaning given that term in section 1030(e) of this title.

"(2) MATERIALLY.—For purposes of paragraphs (3) and (4) of subsection (a), header information or registration information is materially falsified if it is altered or concealed in a manner that would impair the ability of a recipient of the message, an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation.

"(3) MULTIPLE.—The term 'multiple' means more than 100 electronic mail messages during a 24-hour period, more than 1,000 electronic mail messages during a 30-day period, or more than 10,000 electronic mail messages during a 1-year period.

"(4) OTHER TERMS.—Any other term has the meaning given that term by section 3 of the CAN-SPAM Act of 2003."….

(b) UNITED STATES SENTENCING COMMISSION.—

(1) DIRECTIVE.—Pursuant to its authority under section 994(p) of title 28, United States Code, and in accordance with this section, the United States Sentencing Commission shall review and, as appropriate, amend the sentencing guidelines and policy statements to provide appropriate penalties for violations of section 1037 of title 18, United States Code, as added by this section, and other offenses that may be facilitated by the sending of large quantities of unsolicited electronic mail.

(2) REQUIREMENTS.—In carrying out this subsection, the Sentencing Commission shall consider providing sentencing enhancements for—

(A) those convicted under section 1037 of title 18, United States Code, who—

(i) obtained electronic mail addresses through improper means, including—

(I) harvesting electronic mail addresses of the users of a website, proprietary service, or other online public forum operated by another person, without the authorization of such person; and

(II) randomly generating electronic mail addresses by computer; or

(ii) knew that the commercial electronic mail messages involved in the offense contained or advertised an Internet domain for which the registrant of the domain had provided false registration information; and

(B) those convicted of other offenses, including offenses involving fraud, identity theft, obscenity, child pornography, and the sexual exploitation of children, if such offenses involved the sending of large quantities of electronic mail.

(c) SENSE OF CONGRESS.—It is the sense of Congress that—
(1) Spam has become the method of choice for those who distribute pornography, perpetrate fraudulent schemes, and introduce viruses, worms, and Trojan horses into personal and business computer systems; and
(2) the Department of Justice should use all existing law enforcement tools to investigate and prosecute those who send bulk commercial e-mail to facilitate the commission of Federal crimes, including the tools contained in chapters 47 and 63 of title 18, United States Code (relating to fraud and false statements); chapter 71 of title 18, United States Code (relating to obscenity); chapter 110 of title 18, United States Code (relating to the sexual exploitation of children); and chapter 95 of title 18, United States Code (relating to racketeering), as appropriate.

15 U.S.C. § 7704 OTHER PROTECTIONS FOR USERS OF COMMERCIAL ELECTRONIC MAIL. (CAN-SPAM Section 5)

(a) REQUIREMENTS FOR TRANSMISSION OF MESSAGES.—
(1) PROHIBITION OF FALSE OR MISLEADING TRANSMISSION INFORMATION.—It is unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message, or a transactional or relationship message, that contains, or is accompanied by, header information that is materially false or materially misleading. For purposes of this paragraph—

> (A) header information that is technically accurate but includes an originating electronic mail address, domain name, or Internet Protocol address the access to which for purposes of initiating the message was obtained by means of false or fraudulent pretenses or representations shall be considered materially misleading;
> (B) a “from” line (the line identifying or purporting to identify a person initiating the message) that accurately identifies any person who initiated the message shall not be considered materially false or materially misleading; and
> (C) header information shall be considered materially misleading if it fails to identify accurately a protected computer used to initiate the message because the person initiating the message knowingly uses another protected computer to relay or retransmit the message for purposes of disguising its origin.

(2) PROHIBITION OF DECEPTIVE SUBJECT HEADINGS.—It is unlawful for any person to initiate the transmission to a protected computer of a commercial electronic mail message if such person has actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that a subject heading of the message would be likely to mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message (consistent with the criteria used in enforcement of section 5 of the Federal Trade Commission Act (15 U.S.C. 45)).
(3) Inclusion of return address or comparable mechanism in commercial electronic mail—

> (A) IN GENERAL.—It is unlawful for any person to initiate the transmission to a protected computer of a commercial electronic mail message that does not contain a functioning return electronic mail address or other Internet-based mechanism, clearly and conspicuously displayed, that—
>
> > (i) a recipient may use to submit, in a manner specified in the message, a reply electronic mail message or other form of Internet-

based communication requesting not to receive future commercial electronic mail messages from that sender at the electronic mail address where the message was received; and

(ii) remains capable of receiving such messages or communications for no less than 30 days after the transmission of the original message.

(B) MORE DETAILED OPTIONS POSSIBLE.—The person initiating a commercial electronic mail message may comply with subparagraph (A)(i) by providing the recipient a list or menu from which the recipient may choose the specific types of commercial electronic mail messages the recipient wants to receive or does not want to receive from the sender, if the list or menu includes an option under which the recipient may choose not to receive any commercial electronic mail messages from the sender.

(C) TEMPORARY INABILITY TO RECEIVE MESSAGES OR PROCESS REQUESTS.—A return electronic mail address or other mechanism does not fail to satisfy the requirements of subparagraph (A) if it is unexpectedly and temporarily unable to receive messages or process requests due to a technical problem beyond the control of the sender if the problem is corrected within a reasonable time period.

(4) PROHIBITION OF TRANSMISSION OF COMMERCIAL ELECTRONIC MAIL AFTER OBJECTION.—

(A) IN GENERAL.—If a recipient makes a request using a mechanism provided pursuant to paragraph (3) not to receive some or any commercial electronic mail messages from such sender, then it is unlawful—

(i) for the sender to initiate the transmission to the recipient, more than 10 business days after the receipt of such request, of a commercial electronic mail message that falls within the scope of the request;

(ii) for any person acting on behalf of the sender to initiate the transmission to the recipient, more than 10 business days after the receipt of such request, of a commercial electronic mail message with actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that such message falls within the scope of the request;

(iii) for any person acting on behalf of the sender to assist in initiating the transmission to the recipient, through the provision or selection of addresses to which the message will be sent, of a commercial electronic mail message with actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that such message would violate clause (i) or (ii); or

(iv) for the sender, or any other person who knows that the recipient has made such a request, to sell, lease, exchange, or otherwise transfer or release the electronic mail address of the recipient (including through any transaction or other transfer involving mailing lists bearing the electronic mail address of the

recipient) for any purpose other than compliance with this Act or other provision of law.

(B) SUBSEQUENT AFFIRMATIVE CONSENT.—A prohibition in subparagraph (A) does not apply if there is affirmative consent by the recipient subsequent to the request under subparagraph (A).

(5) INCLUSION OF IDENTIFIER, OPT-OUT, AND PHYSICAL ADDRESS IN COMMERCIAL ELECTRONIC MAIL.—

(A) It is unlawful for any person to initiate the transmission of any commercial electronic mail message to a protected computer unless the message provides—

(i) clear and conspicuous identification that the message is an advertisement or solicitation;

(ii) clear and conspicuous notice of the opportunity under paragraph (3) to decline to receive further commercial electronic mail messages from the sender; and

(iii) a valid physical postal address of the sender.

(B) Subparagraph (A)(i) does not apply to the transmission of a commercial electronic mail message if the recipient has given prior affirmative consent to receipt of the message.

(6) MATERIALLY.—For purposes of paragraph (1), the term "materially", when used with respect to false or misleading header information, includes the alteration or concealment of header information in a manner that would impair the ability of an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation, or the ability of a recipient of the message to respond to a person who initiated the electronic message.

(b) Aggravated Violations Relating to Commercial Electronic Mail—

(1) Address harvesting and dictionary attacks—

(A) IN GENERAL.—It is unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message that is unlawful under subsection (a), or to assist in the origination of such message through the provision or selection of addresses to which the message will be transmitted, if such person had actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that—

(i) the electronic mail address of the recipient was obtained using an automated means from an Internet website or proprietary online service operated by another person, and such website or online service included, at the time the address was obtained, a notice stating that the operator of such website or online service will not give, sell, or otherwise transfer addresses maintained by such website or online service to any other party for the purposes of initiating, or enabling others to initiate, electronic mail messages; or

(ii) the electronic mail address of the recipient was obtained using an automated means that generates possible electronic mail

addresses by combining names, letters, or numbers into numerous permutations.

(B) DISCLAIMER.—Nothing in this paragraph creates an ownership or proprietary interest in such electronic mail addresses.

(2) AUTOMATED CREATION OF MULTIPLE ELECTRONIC MAIL ACCOUNTS.—It is unlawful for any person to use scripts or other automated means to register for multiple electronic mail accounts or online user accounts from which to transmit to a protected computer, or enable another person to transmit to a protected computer, a commercial electronic mail message that is unlawful under subsection (a).

(3) RELAY OR RETRANSMISSION THROUGH UNAUTHORIZED ACCESS.—It is unlawful for any person knowingly to relay or retransmit a commercial electronic mail message that is unlawful under subsection (a) from a protected computer or computer network that such person has accessed without authorization.

(c) SUPPLEMENTARY RULEMAKING AUTHORITY.—The Commission shall by regulation, pursuant to section 13—

(1) modify the 10-business-day period under subsection (a)(4)(A) or subsection (a)(4)(B), or both, if the Commission determines that a different period would be more reasonable after taking into account—

(A) the purposes of subsection (a);

(B) the interests of recipients of commercial electronic mail; and

(C) the burdens imposed on senders of lawful commercial electronic mail; and

(2) specify additional activities or practices to which subsection (b) applies if the Commission determines that those activities or practices are contributing substantially to the proliferation of commercial electronic mail messages that are unlawful under subsection (a).

(d) REQUIREMENT TO PLACE WARNING LABELS ON COMMERCIAL ELECTRONIC MAIL CONTAINING SEXUALLY ORIENTED MATERIAL.—

(1) IN GENERAL.—No person may initiate in or affecting interstate commerce the transmission, to a protected computer, of any commercial electronic mail message that includes sexually oriented material and—

(A) fail to include in subject heading for the electronic mail message the marks or notices prescribed by the Commission under this subsection; or

(B) fail to provide that the matter in the message that is initially viewable to the recipient, when the message is opened by any recipient and absent any further actions by the recipient, includes only—

(i) to the extent required or authorized pursuant to paragraph (2), any such marks or notices;

(ii) the information required to be included in the message pursuant to subsection (a)(5); and

(iii) instructions on how to access, or a mechanism to access, the sexually oriented material.

(2) PRIOR AFFIRMATIVE CONSENT.—Paragraph (1) does not apply to the transmission of an electronic mail message if the recipient has given prior affirmative consent to receipt of the message.

(3) PRESCRIPTION OF MARKS AND NOTICES.—Not later than 120 days after the date of the enactment of this Act, the Commission in consultation with the Attorney General shall prescribe clearly identifiable marks or notices to be included in or associated with commercial electronic mail that contains sexually oriented material, in order to inform the recipient of that fact and to facilitate filtering of such electronic mail. The Commission shall publish in the Federal Register and provide notice to the public of the marks or notices prescribed under this paragraph.
(4) DEFINITION.—In this subsection, the term "sexually oriented material" means any material that depicts sexually explicit conduct (as that term is defined in section 2256 of title 18, United States Code), unless the depiction constitutes a small and insignificant part of the whole, the remainder of which is not primarily devoted to sexual matters.
(5) PENALTY.—Whoever knowingly violates paragraph (1) shall be fined under title 18, United States Code, or imprisoned not more than 5 years, or both.

15 U.S.C. § 7705: BUSINESSES KNOWINGLY PROMOTED BY ELECTRONIC MAIL WITH FALSE OR MISLEADING TRANSMISSION INFORMATION. (CAN-SPAM Section 6)

(a) IN GENERAL.—It is unlawful for a person to promote, or allow the promotion of, that person's trade or business, or goods, products, property, or services sold, offered for sale, leased or offered for lease, or otherwise made available through that trade or business, in a commercial electronic mail message the transmission of which is in violation of section 5(a)(1) if that person—

(1) knows, or should have known in the ordinary course of that person's trade or business, that the goods, products, property, or services sold, offered for sale, leased or offered for lease, or otherwise made available through that trade or business were being promoted in such a message;
(2) received or expected to receive an economic benefit from such promotion; and
(3) took no reasonable action—

(A) to prevent the transmission; or
(B) to detect the transmission and report it to the Commission.

(b) Limited Enforcement Against Third Parties—
(1) IN GENERAL.—Except as provided in paragraph (2), a person (hereinafter referred to as the "third party") that provides goods, products, property, or services to another person that violates subsection (a) shall not be held liable for such violation.
(2) EXCEPTION.—Liability for a violation of subsection (a) shall be imputed to a third party that provides goods, products, property, or services to another person that violates subsection (a) if that third party—

(A) owns, or has a greater than 50 percent ownership or economic interest in, the trade or business of the person that violated subsection (a); or
(B)(i) has actual knowledge that goods, products, property, or services are promoted in a commercial electronic mail message the transmission of which is in violation of section 5(a)(1); and
(ii) receives, or expects to receive, an economic benefit from such promotion.

(c) EXCLUSIVE ENFORCEMENT BY FTC.—Subsections (f) and (g) of section 7 do not apply to violations of this section.
(d) SAVINGS PROVISION.—Except as provided in section 7(f)(8), nothing in this section may be construed to limit or prevent any action that may be taken under this Act with respect to any violation of any other section of this Act.

15 U.S.C. § 7706: ENFORCEMENT GENERALLY. (CAN-SPAM Section 7)

(a) VIOLATION IS UNFAIR OR DECEPTIVE ACT OR PRACTICE.—Except as provided in subsection (b), this Act shall be enforced by the Commission as if the violation of this Act were an unfair or deceptive act or practice proscribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(b) ENFORCEMENT BY CERTAIN OTHER AGENCIES….

(c) EXERCISE OF CERTAIN POWERS.—For the purpose of the exercise by any agency referred to in subsection (b) of its powers under any Act referred to in that subsection, a violation of this Act is deemed to be a violation of a Federal Trade Commission trade regulation rule. In addition to its powers under any provision of law specifically referred to in subsection (b), each of the agencies referred to in that subsection may exercise, for the purpose of enforcing compliance with any requirement imposed under this Act, any other authority conferred on it by law.

(d) ACTIONS BY THE COMMISSION.—The Commission shall prevent any person from violating this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act. Any entity that violates any provision of that subtitle is subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act in the same manner, by the same means, and with the same jurisdiction, power, and duties as though all applicable terms and provisions of the Federal Trade Commission Act were incorporated into and made a part of that subtitle.

(e) AVAILABILITY OF CEASE-AND-DESIST ORDERS AND INJUNCTIVE RELIEF WITHOUT SHOWING OF KNOWLEDGE.—Notwithstanding any other provision of this Act, in any proceeding or action pursuant to subsection (a), (b), (c), or (d) of this section to enforce compliance, through an order to cease and desist or an injunction, with section 5(a)(1)(C), section 5(a)(2), clause (ii), (iii), or (iv) of section 5(a)(4)(A), section 5(b)(1)(A), or section 5(b)(3), neither the Commission nor the Federal Communications Commission shall be required to allege or prove the state of mind required by such section or subparagraph.

(f) Enforcement by States—…

(g) Action by Provider of Internet Access Service—
(1) ACTION AUTHORIZED.—A provider of Internet access service adversely affected by a violation of section 5(a)(1), 5(b), or 5(d), or a pattern or practice that violates paragraph (2), (3),

(4), or (5) of section 5(a), may bring a civil action in any district court of the United States with jurisdiction over the defendant—

(A) to enjoin further violation by the defendant; or

(B) to recover damages in an amount equal to the greater of—

(i) actual monetary loss incurred by the provider of Internet access service as a result of such violation; or

(ii) the amount determined under paragraph (3).

(2) SPECIAL DEFINITION OF "PROCURE".—In any action brought under paragraph (1), this Act shall be applied as if the definition of the term "procure" in section 3(12) contained, after "behalf" the words "with actual knowledge, or by consciously avoiding knowing, whether such person is engaging, or will engage, in a pattern or practice that violates this Act".

(3) STATUTORY DAMAGES.—

(A) IN GENERAL.—For purposes of paragraph (1)(B)(ii), the amount determined under this paragraph is the amount calculated by multiplying the number of violations (with each separately addressed unlawful message that is transmitted or attempted to be transmitted over the facilities of the provider of Internet access service, or that is transmitted or attempted to be transmitted to an electronic mail address obtained from the provider of Internet access service in violation of section 5(b)(1)(A)(i), treated as a separate violation) by—

(i) up to $100, in the case of a violation of section 5(a)(1); or

(ii) up to $25, in the case of any other violation of section 5.

(B) LIMITATION.—For any violation of section 5 (other than section 5(a)(1)), the amount determined under subparagraph (A) may not exceed $1,000,000.

(C) AGGRAVATED DAMAGES.—The court may increase a damage award to an amount equal to not more than three times the amount otherwise available under this paragraph if—

(i) the court determines that the defendant committed the violation willfully and knowingly; or

(ii) the defendant's unlawful activity included one or more of the aggravated violations set forth in section 5(b).

(D) REDUCTION OF DAMAGES.—In assessing damages under subparagraph (A), the court may consider whether—

(i) the defendant has established and implemented, with due care, commercially reasonable practices and procedures designed to effectively prevent such violations; or

(ii) the violation occurred despite commercially reasonable efforts to maintain compliance with the practices and procedures to which reference is made in clause (i).

(4) ATTORNEY FEES.—In any action brought pursuant to paragraph (1), the court may, in its discretion, require an undertaking for the payment of the costs of such action, and assess reasonable costs, including reasonable attorneys' fees, against any party.

15 U.S.C. § 7707: EFFECT ON OTHER LAWS. (CAN-SPAM Section 8)

(a) FEDERAL LAW.—(1) Nothing in this Act shall be construed to impair the enforcement of section 223 or 231 of the Communications Act of 1934 (47 U.S.C. 223 or 231, respectively),

chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, United States Code, or any other Federal criminal statute.
(2) Nothing in this Act shall be construed to affect in any way the Commission's authority to bring enforcement actions under FTC Act for materially false or deceptive representations or unfair practices in commercial electronic mail messages.

(b) STATE LAW.—
(1) IN GENERAL.—This Act supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto.
(2) STATE LAW NOT SPECIFIC TO ELECTRONIC MAIL.—This Act shall not be construed to preempt the applicability of—

(A) State laws that are not specific to electronic mail, including State trespass, contract, or tort law; or
(B) other State laws to the extent that those laws relate to acts of fraud or computer crime.

(c) NO EFFECT ON POLICIES OF PROVIDERS OF INTERNET ACCESS SERVICE.—Nothing in this Act shall be construed to have any effect on the lawfulness or unlawfulness, under any other provision of law, of the adoption, implementation, or enforcement by a provider of Internet access service of a policy of declining to transmit, route, relay, handle, or store certain types of electronic mail messages…

16 C.F.R. Part 316: CAN-SPAM Rule

§ 316.2 Definitions….

(m) The definition of the term "sender" is the same as the definition of that term in the CAN-SPAM Act, 15 U.S.C. 7702(16), provided that, when more than one person's products, services, or Internet website are advertised or promoted in a single electronic mail message, each such person who is within the Act's definition will be deemed to be a "sender," except that, only one person will be deemed to be the "sender" of that message if such person: (A) is within the Act's definition of "sender"; (B) is identified in the "from" line as the sole sender of the message; and (C) is in compliance with 15 U.S.C. 7704(a)(1), 15 U.S.C. 7704(a)(2), 15 U.S.C. 7704(a)(3)(A)(i), 15 U.S.C. 7704(a)(5)(A), and 16 CFR 316.4….

(p) "Valid physical postal address" means the sender's current street address, a Post Office box the sender has accurately registered with the United States Postal Service, or a private mailbox the sender has accurately registered with a commercial mail receiving agency that is established pursuant to United States Postal Service regulations.

§ 316.3 Primary purpose.

(a) In applying the term "commercial electronic mail message" defined in the CAN-SPAM Act, 15 U.S.C. 7702(2), the "primary purpose" of an electronic mail message shall be deemed to be commercial based on the criteria in paragraphs (a)(1) through (3) and (b) of this section:[1]

(1) If an electronic mail message consists exclusively of the commercial advertisement or promotion of a commercial product or service, then the "primary purpose" of the message shall be deemed to be commercial.

(2) If an electronic mail message contains both the commercial advertisement or promotion of a commercial product or service as well as transactional or relationship content as set forth in paragraph (c) of this section, then the "primary purpose" of the message shall be deemed to be commercial if:

(i) A recipient reasonably interpreting the subject line of the electronic mail message would likely conclude that the message contains the commercial advertisement or promotion of a commercial product or service; or

(ii) The electronic mail message's transactional or relationship content as set forth in paragraph (c) of this section does not appear, in whole or in substantial part, at the beginning of the body of the message.

(3) If an electronic mail message contains both the commercial advertisement or promotion of a commercial product or service as well as other content that is not transactional or relationship content as set forth in paragraph (c) of this section, then the "primary purpose" of the message shall be deemed to be commercial if:

(i) A recipient reasonably interpreting the subject line of the electronic mail message would likely conclude that the message

[1] The Commission does not intend for these criteria to treat as a "commercial electronic mail message" anything that is not commercial speech.

contains the commercial advertisement or promotion of a commercial product or service; or

(ii) A recipient reasonably interpreting the body of the message would likely conclude that the primary purpose of the message is the commercial advertisement or promotion of a commercial product or service. Factors illustrative of those relevant to this interpretation include the placement of content that is the commercial advertisement or promotion of a commercial product or service, in whole or in substantial part, at the beginning of the body of the message; the proportion of the message dedicated to such content; and how color, graphics, type size, and style are used to highlight commercial content.

(b) In applying the term "transactional or relationship message" defined in the CAN-SPAM Act, 15 U.S.C. 7702(17), the "primary purpose" of an electronic mail message shall be deemed to be transactional or relationship if the electronic mail message consists exclusively of transactional or relationship content as set forth in paragraph (c) of this section.

(c) Transactional or relationship content of email messages under the CAN-SPAM Act is content:

(1) To facilitate, complete, or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender;

(2) To provide warranty information, product recall information, or safety or security information with respect to a commercial product or service used or purchased by the recipient;

(3) With respect to a subscription, membership, account, loan, or comparable ongoing commercial relationship involving the ongoing purchase or use by the recipient of products or services offered by the sender, to provide —

(i) Notification concerning a change in the terms or features;

(ii) Notification of a change in the recipient's standing or status; or

(iii) At regular periodic intervals, account balance information or other type of account statement;

(4) To provide information directly related to an employment relationship or related benefit plan in which the recipient is currently involved, participating, or enrolled; or

(5) To deliver goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender.

§ 316.4 Requirement to place warning labels on commercial electronic mail that contains sexually oriented material.

(a) Any person who initiates, to a protected computer, the transmission of a commercial electronic mail message that includes sexually oriented material must:

(1) Exclude sexually oriented materials from the subject heading for the electronic mail message and include in the subject heading the phrase "SEXUALLY-

EXPLICIT: " in capital letters as the first nineteen (19) characters at the beginning of the subject line;[2]

(2) Provide that the content of the message that is initially viewable by the recipient, when the message is opened by any recipient and absent any further actions by the recipient, include only the following information:

(i) The phrase "SEXUALLY-EXPLICIT:" in a clear and conspicuous manner;[3]

(ii) Clear and conspicuous identification that the message is an advertisement or solicitation;

(iii) Clear and conspicuous notice of the opportunity of a recipient to decline to receive further commercial electronic mail messages from the sender;

(iv) A functioning return electronic mail address or other Internet-based mechanism, clearly and conspicuously displayed, that

(A) A recipient may use to submit, in a manner specified in the message, a reply electronic mail message or other form of Internet-based communication requesting not to receive future commercial electronic mail messages from that sender at the electronic mail address where the message was received; and

(B) Remains capable of receiving such messages or communications for no less than 30 days after the transmission of the original message;

(v) Clear and conspicuous display of a valid physical postal address of the sender; and

(vi) Any needed instructions on how to access, or activate a mechanism to access, the sexually oriented material, preceded by a clear and conspicuous statement that to avoid viewing the sexually oriented material, a recipient should delete the email message without following such instructions.

(b) Prior affirmative consent . Paragraph (a) does not apply to the transmission of an electronic mail message if the recipient has given prior affirmative consent to receipt of the message.

§ 316.5 Prohibition on charging a fee or imposing other requirements on recipients who wish to opt out.

Neither a sender nor any person acting on behalf of a sender may require that any recipient pay any fee, provide any information other than the recipient's electronic mail address and opt-out preferences, or take any other steps except sending a reply electronic mail message or visiting a single Internet Web page, in order to:

[2] The phrase "SEXUALLY-EXPLICIT" comprises 17 characters, including the dash between the two words. The colon (:) and the space following the phrase are the 18th and 19th characters.

[3] This phrase consists of nineteen (19) characters and is identical to the phrase required in 316.5(a)(1) of this Rule.

(a) Use a return electronic mail address or other Internet-based mechanism, required by 15 U.S.C. 7704(a)(3), to submit a request not to receive future commercial electronic mail messages from a sender; or
(b) Have such a request honored as required by 15 U.S.C. 7704(a)(3)(B) and (a)(4).

MySpace, Inc. v. theglobe.com, Inc., 2007 WL 1686966 (C.D. Cal. 2007).
Klausner, District Judge.

…II. FACTUAL BACKGROUND

The following facts are alleged by the parties:

Plaintiff is an online social networking service that allows members to create personal profiles in order to find and communicate with other people. Members of MySpace have access to the MySpace.com website, the MySpace.com Internet Messaging service, and the MySpace.com Mail service, where users can send and receive electronic mail messages ("MySpace e-messages").

To become a MySpace member, a person must set up an account on MySpace.com by creating a profile. The profile includes the user's name, country, zip code, birth date, and gender. The user must also create a password and provide an alternate email address to which confirmations and notifications will be sent. To set up an account, the user must assent to the MySpace Terms of Service Contract ("TOS Contract") by checking a box agreeing to the terms of the TOS Contract, and inputting a verification code. The TOS Contract prohibits spamming, automated use of its system, use of MySpace's service for commercial endeavors, and promotion of information known to be false or misleading.

A MySpace member accesses his e-message account on the internet, at the MySpace.com website. To send a MySpace e-message, the user may either click on a link for "Mail," or go directly to the recipient's unique URL assigned to each individual account.

Defendant is a public company that provides internet-based communications services ("TGLO Products"). Defendant operates one or more websites under various domain names, including iglochat.com, tglophone.com, glotalk.com and digitalvoiceglo.com.

Beginning January 2006, Defendant set up at least 95 identical or virtually identical "dummy" MySpace profiles, with corresponding e-message accounts. Defendant used these accounts to send almost 400,000 unsolicited commercial e-messages marketing TGLO Products to MySpace users via scripts. On February 6, 2006, Plaintiff sent a cease and desist letter to Defendant, demanding that Defendant stop sending its commercial e-messages to MySpace members. Thereafter, Defendant ceased its transmission of e-messages. However, the transmissions later resumed and continued through May 2006.

On June 1, 2006, Plaintiff filed the current action against Defendant. In its Complaint, Plaintiff alleges that Defendant's activities violated both federal and state statutory laws, as well as state common laws. By way of its action, Plaintiff seeks an order enjoining Defendants from the conduct giving rise to Plaintiff's claims. Plaintiff also seeks actual damages, liquidated damages, punitive damages, and attorney's fees and costs….

III. DISCUSSION

At issue in these cross-motions are Count 1 (Violation of CAN-SPAM), Count III (Violation of Section 17529.5) and Count VI (Breach of Contract).

According to Plaintiff, there is no triable issue as to the following alleged facts: Defendant obtained 95 or more MySpace e-message accounts to circumvent MySpace's daily mail limitations. To obtain these accounts, Defendant set up almost 100 separate email accounts at sites such as hotmail.com to fulfill MySpace's requirement of providing an alternate email address. Then, Defendant used false information to set up the MySpace accounts with deceptive display names, and purported to use them for personal purposes. In fact, the accounts were used to initiate (via a script) 399,481 unsolicited commercial email messages to MySpace.com users to promote its TGLO Products. Plaintiff asserts that, as a result of this conduct, partial summary judgment should be granted in its favor as to all three counts.

Defendant contends that: (1) Plaintiff has no standing under CAN-SPAM because it is not an ISP; (2) the messages sent over its private messaging system are not e-mail, and therefore neither CAN-SPAM nor Section 17529.5 apply; and (3) the TOS Contract, in general, is an unenforceable contract of adhesion, and the liquidated damages provision, specifically, is unenforceable because it is disproportionate to anticipated damages.

For the following reasons, the Court denies Defendant's Motion for Partial Summary Judgment, and grants in part, Plaintiff's Motion for Summary Adjudication.

A. Claims Under CAN-SPAM

CAN-SPAM regulates the manner in which unsolicited commercial emails may be transmitted. The statute also makes unlawful certain conduct relating to such transmissions, including the transmission of false or misleading information, and obtaining email addresses through dictionary attacks. Under CAN-SPAM, an Internet access service provider who is harmed by violations of Section 7704(a), (b) or (d) may seek to enjoin further violation by the defendant, or recover damages equal to the greater of: (1) actual monetary loss incurred by the internet access service provider or (2) statutory damages as provided by Section 7706(g)(3)….

1. Plaintiff Has Standing Under CAN-SPAM

As an initial matter, CAN-SPAM, which is primarily a criminal statute, authorizes a private right of action only to a "provider of Internet access service." Defendant contends that Plaintiff is not a provider of Internet access service, and therefore, has no standing to sue Defendant under the statute.

a. Plaintiff is an Internet Access Provider

Under Section 7702(11), "Internet access service" has the meaning given that term in 47 U.S.C. § 231(e)(4) ("Section 231"). Section 231 defines "Internet access service" as "a service that enables users to access content, information, electronic mail, or other services offered over the Internet, and may also include access to proprietary content, information, and other services as part of a package of services offered to consumers."

The Ninth Circuit assumes that the legislative purpose of a statute is expressed by the ordinary meaning of the words used. The plain meaning of the statutory language is unambiguous; "Internet access provider" includes traditional Internet Service Providers ("ISPs"), any email provider, and even most website owners. Under this broad definition, Plaintiff is an "Internet access provider."

b. MySpace E-Messages Are Electronic Mail

Notwithstanding the broad definition given to "Internet access provider," CAN-SPAM provides a private right of action to only those Internet access providers who are adversely affected by Section 7704. Since Section 7704 regulates and prohibits conduct involving electronic mail ("electronic mail" or "email"), a private right of action under CAN-SPAM is confined to only those Internet access services that provide access to electronic mail.

CAN-SPAM defines "electronic mail message" as "a message sent to a unique electronic mail address." "Electronic mail address" is defined as "a destination, commonly expressed as a string of characters, consisting of a unique user name or mailbox (commonly referred to as the 'local part') and a reference to an Internet domain (commonly referred to as the 'domain part'), whether or not displayed, to which an electronic mail message can be sent or delivered."

According to Plaintiff's evidence, the mail of each MySpace user resides at a unique URL, consisting of a string of characters that includes a reference to a user name or number, and the Internet destination, www.myspace.com. This evidence shows that MySpace e-messages fall under CAN-SPAM's definition of electronic mail, and Defendant has failed to present any evidence disputing Plaintiff's evidence.

However, Defendant maintains that MySpace e-messages do not constitute CAN-SPAM protected email because: (1) unlike email, MySpace e-messages have no real "route" because the messages always remain within the "walled garden" of MySpace; (2) MySpace e-messages are not email because they do not use simple mail transfer protocol ("SMTP"); and (3) unlike email addresses, MySpace e-message addresses have no domain part. Defendant's arguments are unavailing.

First, nowhere does the statute specify the requirements set forth by Defendant. Moreover, argument as to these requirements are part and parcel of Defendant's position that only traditional ISPs have a right to sue under CAN-SPAM, as these requirements are typically associated with email service provided by traditional ISPs. As discussed above, the Court rejects this position. Furthermore, CAN-SPAM's Congressional findings indicates that exclusion of electronic messages that fall outside the ambit of Defendant's specifications would subvert the legislative intent. Regardless of who has a private right of action under the statute, the overarching intent of this legislation is to safeguard the convenience and efficiency of the electronic messaging system, and to curtail overburdening of the system's infrastructure. Limiting protection to only electronic mail that falls within the narrows confines set forth by Defendant does little to promote the Congress's overarching intent in enacting CAN-SPAM.

Nonetheless, Plaintiff has introduced evidence showing: (1) its e-message system uses both a routing method and a domain part, and (2) some MySpace e-messages are transmitted using

STMP. First, according to Plaintiff's evidence, every message must contain routing information letting MySpace servers know where to send that message. While the routing employed by MySpace may be less complex and elongated than those employed by ISPs, any routing necessarily implicates issues regarding volume of traffic and utilization of infrastructure-issues which CAN-SPAM seeks to address. Similar to an ISP, there is only a finite volume of mail that MySpace can handle without further investment in infrastructure. Second, Plaintiff's evidence shows that each user's mailbox includes a reference to, not only a user name, but also to myspace.com, the Internet domain or domain part. Finally, Plaintiff's evidence shows that, while most MySpace e-messages are sent using Hypertext Transfer Protocol ("HTTP"), each time an HTTP message is sent by a MySpace user, a companion notification message is sent via SMTP to the recipient's alternative email address. Additionally, MySpace users may send SMTP messages over the Internet from myspace.com when they invite someone who is not a MySpace member to join MySpace. Defendant has not presented any evidence to dispute the evidence set forth above. Therefore, Defendant's argument fails, even under its improperly narrow interpretation of the statute.

Based on the foregoing, the Court finds that Plaintiff has standing to sue Defendant under CAN-SPAM because, as defined under CAN-SPAM, Plaintiff is an Internet access provider whose electronic messages qualify as electronic mail.

2. Violation of Section 7704(a)(1)
Section 7704(a)(1) prohibits the transmission of commercial email that contains false or misleading header information. Under the statute, even if the header information is technically accurate, it is considered materially misleading if it includes an originating email address that was accessed through false or fraudulent pretenses, for purposes of initiating the commercial email message.

According to Plaintiff's evidence, Defendant's employees created MySpace accounts using false identifying information, including fictitious email addresses and contact information. Defendant's employees also set up MySpace accounts with the display names, "MySpace Phone," "Chick," and "Coppermine." As indicated by this evidence, the accounts created by Defendant failed to identity the messages as originating from TheGlobe. Based on the plain language of Section 7704(a)(1), Plaintiff's evidence establishes that Defendant violated this provision.

In opposition, Defendant argues that the accounts did, in fact, identify TheGlobe as the originator of the e-messages. To support its argument, Defendant has introduced evidence that a document was used to assist employees in creating MySpace accounts. According to this evidence, the document instructed the employees to use "tglo" in the first name and "phone" as the last name. This evidence is unavailing, as it fails to dispute Plaintiff's evidence or otherwise support its proposition. At most, the evidence indicates that, in addition to the false accounts described by Plaintiff's evidence, some of Defendant's other accounts may have had as their account identifiers the words "tglo" and "phone," the product Defendant sought to market. Even so, this fact is irrelevant because Defendant has not offered any evidence showing that those words are readily associated with TheGlobe or its TGLO Products. As such, the Court finds no triable issue as to Defendant's violation of Section 7704(a)(1).

3. Violation of Section 7704(a)(2)
Section 7704(a)(2) prohibits a person from transmitting commercial email containing a subject heading that he or she knows would likely mislead the recipient about a material fact regarding the content or subject matter of the message. Under Section 7706(g)(1), a private right of action under Section 7704(a)(2) is available only when there is a pattern or practice that violates this provision.

It is undisputed that Defendant sent MySpace e-messages with the subject headings, “the new MySpace phone,” “the new phone for MySpace,” and “the new tglo phone for MySpace.” The last heading does not violate the statute, as it references “tglo” in a way that accurately describes the content of the message and implies a product that is separate and distinct from MySpace. In contrast, the first two headings do violate the statute because they imply an affiliation with MySpace, likely misleading the recipient into believing that the marketed product is related to MySpace. In fact, it is undisputed that in late January 2006, an influential technology blogger on Zdnet.com inaccurately reported that MySpace had partnered with TheGlobe. Although Defendant was aware of this error, it never sought to correct the misinformation. Significantly, the undisputed evidence shows that the subject headings described above were attached to e-messages sent after Defendant learned of the blogger’s inaccurate report. As such, the Court finds that Defendant knew, or should have known, that its subject headings were misleading.

Defendant argues that Plaintiff fails to show a pattern or practice. As to this provision, the Court agrees. The undisputed evidence shows that Defendant’s employees were provided written instructions on how to create MySpace accounts and what content to send through the messaging system. The instructions directed the employees to use “Call for FREE fast and easy” as the headline. This subject heading is consistent with the email content, and does not violate Section 7704(a)(2). As discussed above, notwithstanding the written instructions, as least a portion of the 399,481 e-messages sent by Defendant contained deceptive subject headings that violated the statute. However, without further evidence as to the number of such e-messages sent by Defendant, it is impossible to determine whether Defendant’s violation of this provision rose to the level of a pattern or practice. Therefore, a triable issue of fact exists as to whether the number of e-messages containing deceptive subject headings is substantial enough to constitute a pattern or practice.

4. Violation of Section 7704(a)(5)
Section 7704(a)(5) requires that unsolicited commercial emails contain: (1) clear notification that the message is an advertisement, (2) clear notice of the opportunity to decline receipt of further messages from the sender, and (3) a valid physical postal address for the sender. Again, under Section 7706(g)(1), a private right of action under Section 7704(a)(5) is available only when the defendant has a pattern or practice of violating this provision.

It is undisputed that none of Defendant’s 399,481 e-messages contained clear notice of the opportunity to decline receipt of further messages from the sender, or a valid physical postal address for the sender. Therefore, Defendant clearly violated this statutory provision.

Again, Defendant argues that its activities do not constitute a pattern or practice, as prescribed by Section 7706(g)(1). However, as stated above, the following is undisputed: (1) Defendant's employees were given instructions on how to create a MySpace account, what information should be placed in the profiles, and what content to write in the messages; and (2) through its employees, Defendant created at least 95 MySpace accounts and sent 399,481 unsolicited commercial emails over a course of five months. This evidence shows that, rather than an isolated or accidental event, Defendant sent these e-messages in a regular and repeated fashion, as a part of Defendant's marketing practice. Since each one of the 399,481 messages violated Section 7704(a)(5), Plaintiff has shown that Defendant engaged in a pattern or practice of violating this provision. As such, the Court finds no triable issue of fact as to Defendant's liability for violation of Section 7704(a)(5).

5. Violation of Section 7704(b)(1)

Section 7704(b) makes it an aggravated violation to initiate the transmission of commercial email that is unlawful under Section 7704(a) where "the electronic mail address of the recipient was obtained using an automated means that generates possible electronic mail addresses by combining names, letter or numbers into numerous permutation."

Plaintiff's evidence shows that Defendant randomly selected a range of MySpace ID numbers. Defendant then used a script to automatically generate a set of sequential IDs. Once these IDs were generated, the script automatically transmitted Defendant's messages to those IDs. According to the evidence, some of the IDs correlated to MySpace profiles, and some did not. A total of 399,481 messages were sent using this script. Based on the evidence presented, Defendant violated Section 7704(1)(A)(ii).

In opposition, Defendant argues that it did not violate the statutory provision because the script sent messages in sequence, rather than at random. Defendant further argues that the script sent the messages to a range of MySpace profiles by using a range of user IDSs that had already been assigned by MySpace. Defendant's arguments are unavailing, as it is unclear how these distinctions change the fact that Defendant used "automated means that generates possible electronic mail addresses." As such, the Court finds no triable issue as to Defendant's violation of Section 7704(b)(1)(A)(ii).

B. Section 17529.5 Claim

Section 17529.5 prohibits email transmissions to or from California email addresses containing "falsified, misrepresented or forged header information" or a subject line that would likely "mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message." Under the statute, an electronic mail service provider[7] may bring an action against a person or entity that violates this section.

It is undisputed that MySpace's servers, which house all MySpace.com e-message accounts, are located in California. Furthermore, it is undisputed that every time a user logs on to

[7] An "electronic mail service provider" is defined as "any person, including an Internet service provider, that is an intermediary in sending or receiving electronic mail or that provides to end users of the electronic mail service the ability to send or receive electronic mail."

MySpace.com to send, review or reply to an e-message, he or she is doing so by accessing the California servers. Based on this evidence, as well as the evidence and analysis discussed in Section III.A. above, the Court finds no triable issues as to Defendant's liability for Plaintiff's Section 17529.5 claim.

C. Breach of Contract Claim

To set up a MySpace account, a person must assent to the TOS Contract by checking a box agreeing to its terms. Plaintiff claims that, by setting up 95 accounts and sending its marketing e-messages through those accounts, Defendant breached the terms of the TOS Contract. Furthermore, due to modified terms of the TOS Contract, Plaintiff contends that Defendant must pay $50 for each of its e-messages that were sent after March 17, 2006.

1. Breach of the TOS Contract

It is undisputed that Defendant's e-messages were sent between January 2006 and May 2006. During that time, the TOS Contract was modified three times. All four versions of the TOS Contract contain the following provision: MySpace is "for the personal use of Members only and may not be used in connection with any commercial endeavors except those that are specifically endorsed or approved by the management of MySpace.com. Also, each version prohibits: (1) content that involves the transmission of 'junk mail,' 'chain letters," or unsolicited mass mailing or 'spamming;' and (2) "any automated use of the system, such as using scripts to add friends."

Based on the evidence and analysis discussed in Section III.A above, the Court finds that Defendant used a script to transmit an unsolicited mass mailing to MySpace users for purposes of an unapproved commercial endeavor. This activity violates the terms of the TOS Contract.

Defendant argues that the TOS Contract, as a whole, is entirely unenforceable because every relevant version is a contract of adhesion, such that the terms are unconscionable. This argument is not well-taken.

The doctrine of unconscionability provides that a contract is unenforceable if it is both procedurally and substantively unconscionable. Procedural unconscionability focuses on oppression and surprise due to unequal bargaining power. "Oppression" arises from the inequality of the parties' bargaining power and an absence of real negotiation or a meaningful choice on the weaker party's part. "Surprise" is found when "the terms to which the party supposedly agreed [are] hidden in a prolix printed form drafted by the party seeking to enforce them." A contract is substantively unconscionable when its terms are so harsh, oppressive, or one-sided as to shock the conscience.

A review of the TOS Contract shows that it is, in fact, a standardized contract that gives the subscribing party only the opportunity to adhere to the contract or reject it. However, the facts indicate that Defendant had a reasonable alternative or meaningful choice in the matter, in that marketing through MySpace using the method employed was not its only choice. In fact, Plaintiff's evidence shows that Defendant had, in fact, considered purchasing advertising space on the MySpace website. Moreover, the Court finds that the contract is not written prolixly, particularly for an experienced, sophisticated business entity whose area of expertise involves

Internet related technology. Even if the TOS contract was procedurally unconscionable, the terms, as a whole, are certainly not so harsh, oppressive, or one-sided as to shock the conscience.

In light of the above, the Court finds that Defendant breached the TOS Contract.

2. Liquidated Damages Provision

On March 17, 2006, Plaintiff modified the TOS Contract and included the following provision: "Prohibited activity includes ... advertising to, or solicitation of, any Member to buy or sell any products or services through the Services. If you breach this Agreement and send unsolicited bulk email, ... or other unsolicited communications of any kind ... As a reasonable estimation of such harm, you agree to pay MySpace.com $50 for each such unsolicited email ... you send through the Services;...."

Plaintiff asserts that, under this provision, Defendant is liable for liquidated damages in the amount of $50 per message sent after March 17, 2006. Defendant argues that the $50 liquidated damages clause is unenforceable because it is an impermissible contractual penalty. The Court disagrees.

California law provides that liquidated damages clauses are enforceable where: (1) damages from a breach would be impracticable or extremely difficult to determine with certainty; and (2) the amount represents a reasonable estimation of what such damages might be. As stated above, the Court has found that Defendant breached the TOS Agreement by bulk transmission of unapproved, unsolicited commercial e-messages. The costs associated with this activity include not only infrastructure costs, such as additional bandwidth, and monitoring costs, they are also rife with large hidden costs. Such hidden costs include those associated with deterrence (legal fees, software, etc.), depletion of customer goodwill, and liability implications associated with the unlawfully advertised product. Therefore, the damages related to Defendant's breach are, in fact, impracticable or extremely difficult to determine. As to the amount of liquidated damages, CAN-SPAM sets statutory damages for unsolicited commercial emails at $25-$300 per message. Moreover, while the costs associated with spamming are difficult to definitively assess, the costs listed above are certainly large, and only the tip the iceberg. Therefore, the Court finds $50 per message a reasonable estimation of Plaintiff's damages.

Defendant further argues that, even if the Court finds the liquidated provision enforceable, the provision should be applied only to those messages that were sent from accounts created after March 17, 2006. Plaintiff contends that, because the TOS contract specifically provides for modification of the agreement, the provision should apply to all messages sent after March 17, 2006, regardless of when the account was created. The Court agrees with Plaintiff.

All four versions of the TOS Contract specifically provide: "MySpace.com may modify this Agreement from time to time and such modification shall be effective upon posting by MySpace.com on the Website. *You agree to be bound to any changes to this Agreement when you use the Service after any such modification is posted*." (emphasis added). For the same reasons stated above, this contractual term is neither procedurally nor substantively unconscionable. Additionally, the Court notes that Defendant created all 95 MySpace accounts, both before and after March 17, 2006. Therefore, at the time it created its post-March 17

accounts, it knew, or should have known, that all messages, even those sent from pre-March 17 accounts, were subject to the liquidated damages provision. As such, the Court finds that the liquidated damages provision contained in the March 17, 2006 TOS Contract applies to all messages sent by Defendant after March 17, 2006….

Omega World Travel, Inc. v. Mummagraphics, Inc., 469 F.3d 348 (4th Cir. 2006).
Wilkinson, Circuit Judge.

Countless commercial e-mail messages, known colloquially as "spam," pass through the Internet every day, inspiring frustration, countermeasures, and—as here—lawsuits. Based upon eleven commercial e-mail messages, Mummagraphics, Inc., a provider of online services, seeks significant statutory damages from Omega World Travel, Inc., a Virginia-based travel agency ("Omega"); Gloria Bohan, Omega's president and founder; and Cruise.com, Inc., a wholly owned subsidiary of Omega (collectively, "appellees"). Mummagraphics alleges that Cruise.com sent the messages in violation of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM Act"), 15 U.S.C. §§ 7701 et seq., as well as Oklahoma law.

The district court awarded summary judgment to the appellees on all of Mummagraphics' claims and we affirm. The CAN-SPAM Act preempts Mummagraphics' claims under Oklahoma's statutes. In addition, Mummagraphics failed to allege the material inaccuracies or pattern of failures to conform to opt-out requirements that is necessary to establish liability under the CAN-SPAM Act. The CAN-SPAM Act addresses "spam" as a serious and pervasive problem, but it does not impose liability at the mere drop of a hat.

I.

Appellant Mummagraphics, Inc., d/b/a Webguy Internet Solutions, is an Oklahoma corporation with its only place of business in Oklahoma City. According to Mark Mumma, the company's president, Mummagraphics hosts web pages, registers domain names, designs web pages and logos, and sets up computer servers. Mummagraphics also operates websites devoted to opposing "spam" messages including "sueaspammer.com." In addition, Mummagraphics runs a website, "OptOutByDomain.com," that lists Internet domain names—roughly seventy of 347 of which are operated by Mummagraphics—whose owners have indicated that they do not wish to receive unsolicited commercial e-mail messages. Mummagraphics owns the domain name webguy.net and uses the e-mail account inbox@webguy.net for company purposes.

Cruise.com operates a website selling cruise vacations and sends e-mail advertisements—dubbed "E-deals"—to prospective customers. It sent eleven "E-deals" containing travel offers to inbox@webguy.net between December 29, 2004 and February 9, 2005. Each message contained a line of text on which the recipient could click in order to be removed from future mailings, and each message also said that the recipient could opt-out of future e-mails by writing to a postal address contained in each message. Each message also contained a link to the Cruise.com website and a toll-free phone number for the company.

Mummagraphics claims that the messages contained several inaccuracies. First, each message stated that the recipient had signed up for the Cruise.com mailing list, but Mummagraphics alleges that it had not asked that inbox@webguy.net receive the company's offers. Second, while each message listed Cruise.com as the sending organization, each also included the address "FL-Broadcast.net" in its header information, even though Mummagraphics alleges that "FL-Broadcast.net" is not an Internet domain name linked to Cruise.com or the other appellees. In

addition, the messages contained the "from" address cruisedeals@cruise.com, even though Cruise.com had apparently stopped using that address.

When Mark Mumma noticed the Cruise.com e-mails that inbox@webguy.net had received, he did not use the electronic opt-out link to remove the address from the Cruise.com e-mail list, but instead called John Lawless, Omega World Travel's general counsel, to complain. Mumma told Lawless that he had not asked to receive the "E-deal" messages. He told Lawless that he refused to use e-mail opt-out mechanisms because "only idiots do that," and he believed opt-out mechanisms just led to more unwanted messages. Mumma told Lawless that his preferred removal procedure was to sue for violations of Oklahoma law. Lawless asked Mumma for his e-mail address, but Mumma did not provide it. Instead, he asked Lawless to remove from all future mailings every address containing a domain name listed on Mummagraphics' "OptOutByDomain.com" website. Lawless said he was "gonna take them down right now," but Omega's technical support division indicated that removing all the addresses would require considerable effort, and the addresses were not immediately removed.

On January 20, 2005, the day after speaking with Lawless, Mumma received another "E-deal" message at inbox@webguy.net. He sent a letter dated January 25, 2005 to Daniel Bohan of Omega World Travel, saying that he had received six unsolicited "E-deal" messages from Cruise.com, Omega's subsidiary, but again not specifying the e-mail address at which he had received the messages. The letter claimed that the messages violated federal and state laws and said that Mumma intended to sue Bohan's company for at least $150,000 in statutory damages unless Bohan settled the matter for $6,250. Mumma attached the Cruise.com e-mails to his letter, and after John Lawless noticed that the messages appeared to have been sent to inbox@webguy.net, he directed that the address be removed from the Cruise.com mailing list. The company subsequently removed the address.

After Omega World Travel failed to pay Mumma, postings on one of Mumma's "anti-spam" websites accused Omega, Cruise.com, and Daniel and Gloria Bohan of being "spammers" who had violated state and federal laws. The website posted a photo of the Bohans that had evidently been copied from the Omega website and described the couple as "cruise.com spammers." On the basis of these postings, Omega World Travel, the Bohans, and Cruise.com sued Mumma and Mummagraphics in federal court, claiming defamation, copyright infringement, trademark infringement, and unauthorized use of likeness. The district court granted Mummagraphics summary judgment on all these claims except the libel action, on which all the plaintiffs except Daniel Bohan, who is no longer a party, expect to proceed to trial.

Mummagraphics raised counterclaims against the appellees under Oklahoma and federal law, which are the only claims now before this court. Mummagraphics alleged, inter alia, that the Cruise.com e-mails contained actionable inaccuracies and that the appellees failed to comply with federal and state requirements that they stop sending messages to recipients who opted out through specified procedures. Both parties sought summary judgment on Mummagraphics' counterclaims, and the district court granted the appellees' motion. The court held that the CAN-SPAM Act preempted Mummagraphics' claims under Oklahoma's statutes. It further held, *inter alia*, that the appellees had not violated the CAN-SPAM Act because the alleged e-mail

inaccuracies were not material and the appellees had not violated the opt-out provisions. Mummagraphics now appeals.

II.

A.

We turn first to the district court's determination that the CAN-SPAM Act preempted Mummagraphics' claims under Oklahoma's statutes regulating commercial e-mail messages. The basic principles of preemption are well settled, and we need not belabor them here. Our inquiry into the scope of a preemption clause is shaped by "two presumptions." First, under our federal system, we do not presume that Congress intends to clear whatever field it enters. Instead, we start from "the basic assumption that Congress did not intend to displace state law," and "that the historic police powers of the States were not to be superseded by the Federal Act unless that was the clear and manifest purpose of Congress." Second, from this departure point, we address preemption issues in accordance with the "oft-repeated comment ... that '[t]he purpose of Congress is the ultimate touchstone' in every preemption case." Instead of imposing the narrowest possible construction on preemptive language when read in isolation, we seek "a fair understanding of congressional purpose," looking to "the language of the pre-emption statute and the statutory framework surrounding it," while also considering "the structure and purpose of the statute as a whole."

B.

Mummagraphics argues that it is entitled to damages because such damages are authorized by Oklahoma law and lie outside the CAN-SPAM Act's preemptive scope. The CAN-SPAM Act provides, in part,

> This chapter supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto.

The principal Oklahoma provision under which Mummagraphics seeks damages provides:

> It shall be unlawful for a person to initiate an electronic mail message that the sender knows, or has reason to know:
>
> 1. Misrepresents any information in identifying the point of origin or the transmission path of the electronic mail message;
>
> 2. Does not contain information identifying the point of origin or the transmission path of the electronic mail message; or
>
> 3. Contains false, malicious, or misleading information which purposely or negligently injures a person.

Okla. Stat. tit. 15, § 776.1A.[1]

Oklahoma courts appear not to have construed the state provision, but the language seems to reach beyond common law fraud or deceit. By its terms, the statute is not limited to inaccuracies in transmission information that were material, led to detrimental reliance by the recipient, and were made by a sender who intended that the misstatements be acted upon and either knew them to be inaccurate or was reckless about their truth.

The district court held that the Oklahoma statutes were preempted insofar as they applied to immaterial misrepresentations, and that this ruling disposed of Mummagraphics' Oklahoma statutory claims. Mummagraphics does not challenge the district court's reading of Oklahoma law or Mummagraphics' complaint, but it argues that the district court was incorrect to hold actions for immaterial error to be preempted because the CAN-SPAM Act permits states to "prohibit[ ] falsity or deception."

Whatever the precise scope of the Oklahoma provision might be, we cannot agree that Mummagraphics' action for immaterial errors survives preemption. To begin with, the language in the exception to the federal preemption provision upon which Mummagraphics relies is hardly as straightforward as the company suggests. The exception, as noted, allows states to prohibit "falsity or deception" in commercial e-mail messages. Those terms are not defined in the statute. However, "deception" requires more than bare error, and while "falsity" can be defined as merely "the character or quality of not conforming to the truth or facts," it also can convey an element of tortiousness or wrongfulness, as in "deceitfulness, untrustworthiness, faithlessness." Webster's Third New International Dictionary Unabridged 820 (1971); see also Oxford English Dictionary Vol. V 697 (2d ed. 1989) (defining false as "erroneous, wrong," but also as "mendacious, deceitful, treacherous," and "[p]urposely untrue"); see also Black's Law Dictionary 635 (8th ed. 2004) (defining "false" as "untrue" but also as "deceitful; lying").

Since the word "falsity" considered in isolation does not unambiguously establish the scope of the preemption clause, we read "falsity" in light of the clause as a whole. Reading "falsity" as referring to traditionally tortious or wrongful conduct is the interpretation most compatible with the maxim of *noscitur a sociis*, that a word is generally known by the company that it keeps. The canon applies in the context of disjunctive lists. Here, the pre-emption clause links "falsity" with "deception"—one of the several tort actions based upon misrepresentations. Keeton et al., Prosser and Keeton on the Law of Torts § 105, at 726-27 (5th ed. 1984) (defining deceit as species of false-statement tort); Restatement (Second) of Torts § 525 (describing elements of deceit). This pairing suggests that Congress was operating in the vein of tort when it drafted the pre-emption clause's exceptions, and intended falsity to refer to other torts involving misrepresentations, rather than to sweep up errors that do not sound in tort.

[1] Mummagraphics also alleged that the appellees violated an Oklahoma provision requiring senders of unsolicited commercial e-mails to comply with certain opt-out requests. We agree with the district court that this provision was preempted because it bears no arguable relationship to the subject matter excepted from preemption in the CAN-SPAM Act. Finally, Mummagraphics alleged that the appellees violated the Oklahoma Consumer Protection Act by violating Oklahoma's commercial e-mail laws. Since we find that Mummagraphics did not raise a cognizable cause of action under Oklahoma's commercial e-mail laws due to federal preemption, the alleged violations cannot give rise to further claims under the Oklahoma Consumer Protection Act.

Other sections of the CAN-SPAM Act do not support a bare-error reading of "falsity." In the portion of the Act that created a civil cause of action, Congress affixed the title "[p]rohibition of false or misleading transmission information" to a section that prohibits only "header information that is *materially* false or *materially* misleading." (emphasis added). While "the heading of a section cannot limit the plain meaning of the text," it can "shed light on some ambiguous word or phrase." Moreover, the "normal rule of statutory construction" provides that "identical words used in different parts of the same act are intended to have the same meaning." Whether linked with materiality or "deception," we can find nowhere in the statute that Congress meant to apply falsity in a mere error sense.

There are good reasons for this. Congress did not intend "falsity" to encompass bare error because such a reading would upset the Act's careful balance between preserving a potentially useful commercial tool and preventing its abuse. The Act's enacted findings make clear that Congress saw commercial e-mail messages as presenting both benefits and burdens. Congress found that "[t]he convenience and efficiency of electronic mail are threatened by the extremely rapid growth in the volume of unsolicited commercial electronic mail," but also that e-mail's "low cost and global reach make it extremely convenient and efficient, and offer unique opportunities for the development and growth of frictionless commerce." Congress noted that states had sought to regulate commercial e-mails, but it found that the resulting patchwork of liability standards had proven ineffective:

> Many States have enacted legislation intended to regulate or reduce unsolicited commercial electronic mail, but these statutes impose different standards and requirements. As a result, they do not appear to have been successful in addressing the problems associated with unsolicited commercial electronic mail, in part because, since an electronic mail address does not specify a geographic location, it can be extremely difficult for law-abiding businesses to know with which of these disparate statutes they are required to comply.

Congress implemented these findings by creating a national standard that would be undermined to the point of near-irrelevancy by Mummagraphics' interpretation of the preemption clause. Rather than banning all commercial e-mails or imposing strict liability for insignificant inaccuracies, Congress targeted only e-mails containing something more than an isolated error. The CAN-SPAM Act made it a crime to "materially falsif[y] header information in multiple commercial electronic mail messages and intentionally initiate[ ] the transmission of such messages," but it attached no criminal sanction to non-material errors. The Act created civil causes of action relating to error, but attached requirements beyond simple mistake to each of them. It permitted lawsuits based upon "*materially* false or *materially* misleading" header information. (emphasis added). The Act made it actionable for a person to "initiate the transmission to a protected computer of a commercial electronic mail message if such person has *actual knowledge, or knowledge fairly implied on the basis of objective circumstances,* that a subject heading of the message would be *likely to mislead a recipient*, acting reasonably under the circumstances, about a *material* fact regarding the contents or subject matter of the message...." (emphasis added). In sum, Congress' enactment governing commercial e-mails reflects a calculus that a national strict liability standard for errors would impede "unique

opportunities for the development and growth of frictionless commerce," while more narrowly tailored causes of action could effectively respond to the obstacles to "convenience and efficiency" that unsolicited messages present.

Mummagraphics' reading of the preemption clause would upend this balance and turn an exception to a preemption provision into a loophole so broad that it would virtually swallow the preemption clause itself. While Congress evidently believed that it would be undesirable to make all errors in commercial e-mails actionable, Mummagraphics' interpretation would allow states to bring about something very close to that result.

The ensuing consequences would undermine Congress' plain intent. As we have noted, Congress found that because e-mail addresses do not specify recipients' physical locations, it can be difficult or impossible to identify where recipients live and hence to determine the state laws that apply. Moreover, commercial e-mails are a bulk medium used to target thousands of recipients with a single mouse-click, meaning that the typical message could well be covered by the laws of many jurisdictions. As a result, law-abiding senders would likely have to assume that their messages were governed by the most stringent state laws in effect. The strict liability standard imposed by a state such as Oklahoma would become a de facto national standard, with all the burdens that imposed, even though the CAN-SPAM Act indicates that Congress believed a less demanding standard would best balance the competing interests at stake. Because Mummagraphics' reading of the "falsity or deception" exception would thus permit an exception to preemption to swallow the rule and undermine the regulatory balance that Congress established, Mummagraphics' reading of the exception is not compatible with the structure of the CAN-SPAM Act as a whole.

C.

By giving the preemption provision its proper scope, we avoid the need to resolve a difficult constitutional question concerning the compatibility of Oklahoma's commercial e-mail provisions with the dormant commerce clause. Congress' power to regulate interstate commerce implicitly prohibits states from passing any law that "discriminates against or unduly burdens interstate commerce and thereby 'imped[es] free private trade in the national marketplace.'" Whether a nondiscriminatory law unduly burdens interstate commerce turns upon whether it serves a "legitimate local purpose," and, if so, "the nature of the local interest involved, and ... whether it could be promoted as well with a lesser impact on interstate activities."

This is not a simple case because important interests lie on both sides of the *Pike* analysis. We have previously deemed it relevant that one state's Internet laws may impose compliance costs on businesses throughout the country, because it is difficult for businesses to determine where Internet users are located. Moreover, courts have long recognized that civil liability for false statements can burden even innocent speech. The deterrent effect on commercial speech would be particularly great under a statute that authorizes enormous statutory damages—$25,000 for each day of violations. On the other hand, false and misleading content on the Internet is a serious problem, and even innocent inaccuracies can impose costs that states may view as a

proper object of redress. We avoid a difficult balancing analysis by giving Congress' preemption clause its proper scope.[2]

III.

We turn next to Mummagraphics' claims that the Cruise.com e-mails violated the CAN-SPAM Act.[3] Mummagraphics first argues that the Cruise.com e-mails violated the Act's requirements concerning the accuracy of header information in commercial e-mails. The Act provides, "It is unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message ... that contains, or is accompanied by, header information that is materially false or materially misleading." The Act further explains,

> the term "materially", when used with respect to false or misleading header information, includes the alteration or concealment of header information in a manner that would impair the ability of an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation, or the ability of a recipient of the message to respond to a person who initiated the electronic message.

Mummagraphics alleges that the senders of the Cruise.com e-mails violated this provision because the messages' header information incorrectly indicated that the e-mails originated from the server "FL-Broadcast.net," and because the messages' "from" address read cruisedeals@cruise.com, although that e-mail address was apparently non-functional.

We agree with the district court that these inaccuracies do not make the headers "materially false or materially misleading." The e-mails at issue were chock full of methods to "identify, locate, or respond to" the sender or to "investigate [an] alleged violation" of the CAN-SPAM Act. Each message contained a link on which the recipient could click in order to be removed from future mailings, in addition to a separate link to Cruise.com's website. Each message prominently displayed a toll-free number to call, and each also listed a Florida mailing address and local phone number for the company. Several places in each header referred to the Cruise.com domain name, including one line listing Cruise.com as the sending organization.

These references come as little surprise, because the "E-deal" messages were sales pitches intended to induce recipients to contact Cruise.com to book the cruises that the messages advertised. Since the "E-deal" messages and their headers were replete with accurate identifiers of the sender, the alleged inaccuracies in the headers could not have impaired the efforts of any recipient, law enforcement organization, or other party raising a CAN-SPAM claim to find the company. If the alleged inaccuracies in a message containing so many valid identifiers could be described as "materially false or materially misleading," we find it hard to imagine an inaccuracy

[2] Giving the preemption clause its proper scope also allows us to avoid deciding whether such a stringent liability statute exceeds even the states' wide latitude to regulate false or misleading commercial speech.

[3] We shall assume without deciding that Mummagraphics qualifies as an Internet Access Service Provider entitled to bring a claim under the CAN-SPAM Act.

that would not qualify as "materially false or materially misleading." Congress' materiality requirement would be rendered all but meaningless by such an interpretation.

We also reject Mummagraphics' claim for alleged violations of the CAN-SPAM Act's e-mail removal provisions, because Mummagraphics cannot sustain such a claim without evidence that could establish a "pattern or practice" of violations. The CAN-SPAM Act requires that the commercial e-mails it covers include

> a functioning return electronic mail address or other form of Internet-based mechanism, clearly and conspicuously displayed, that ... a recipient may use to submit, in a manner specified in the message, a reply electronic mail message or other form of Internet-based communication requesting not to receive future commercial electronic mail messages from that sender at the electronic mail address where the message was received....

Senders must honor requests for removal made using these mechanisms within ten business days. While the Act permits Internet access service providers to bring suit under these provisions, they may do so only for "a pattern or practice" that violates the requirements. In this case, Mummagraphics merely alleged that the appellees failed to remove inbox@webguy.net from the "E-deals" mailing list within ten days of Mark Mumma's call to Omega's general counsel. It does not allege that the appellees failed to comply with any other removal request. As a result, Mummagraphics has not alleged facts sufficient to survive summary judgment on its opt-out claim. This holding makes it unnecessary to address the district court's ruling that Mummagraphics' evidence did not point to even a single violation of the CAN-SPAM Act's opt-out provisions.

IV.

Lastly, Mummagraphics claims that Cruise.com's e-mail messages amounted to trespass to chattels under Oklahoma law. While the CAN-SPAM Act does not preempt the application of state tort laws that are not specific to e-mail messages, the district court correctly granted summary judgment on this claim because Mummagraphics has not offered evidence that Cruise.com's e-mails caused the company more than nominal damages. Trespass to chattel is a common law tort that "may be committed by intentionally (a) dispossessing another of the chattel, or (b) using or intermeddling with a chattel in the possession of another." However, trespass to chattel claims may be brought against a trespasser only if

> (a) he dispossesses the other of the chattel, or
> (b) the chattel is impaired as to its condition, quality or value, or
> (c) the possessor is deprived of the use of the chattel for a substantial time, or
> (d) bodily harm is caused to the possessor, or harm is caused to some person or thing in which the possessor has a legally protected interest.

Restatement (Second) of Torts § 218. We proceed with particular caution in this area because Oklahoma courts appear never to have recognized this tort based upon intangible invasions of

computer resources. In fact, the *Woodis* court described "intermeddling" with a chattel as meaning "intentionally bringing about a physical contact with the chattel."

Even if Oklahoma law were to make trespass against chattels available for computer intrusions, Mummagraphics' claim cannot survive summary judgment because the courts that recognize trespass to chattels based upon computer intrusions do not allow "an action for nominal damages for harmless intermeddlings with the chattel." Intel Corp. v. Hamidi, 30 Cal.4th 1342 (2003) (quoting Restatement (Second) of Torts § 218 cmt. e (1965)). Because Mummagraphics failed to submit any evidence that the receipt of eleven commercial e-mail messages placed a meaningful burden on the company's computer systems or even its other resources, summary judgment was appropriate on this counterclaim.

V.

We respect the fact that unsolicited commercial e-mail has created frustration and consternation among innumerable users of the Internet. The proper treatment of mass commercial e-mail has provoked controversy since perhaps the first such message was sent. Our role is not to determine the best way of regulating such messages, but merely to implement the balance that Congress struck. The CAN-SPAM Act prohibits some material misstatements and imposes opt-out requirements, but it does not make every error or opt-out request into grounds for a lawsuit. The e-mails in this case are not actionable under the Act. Nor can the messages be actionable under Oklahoma's statutes, because allowing a state to attach liability to bare immaterial error in commercial e-mails would be inconsistent with the federal Act's preemption text and structure, and, consequently, with a "fair understanding of congressional purpose." Since we agree that summary judgment was warranted on Mummagraphics' various claims, the judgment of the district court is

AFFIRMED.

The Third Wave of Internet Exceptionalism
By Eric Goldman
Posted March 11, 2009 to http://blog.ericgoldman.org/archives/2009/03/the_third_wave.htm

From the beginning, the Internet has been viewed as something special and "unique." For example, in 1996, a judge called the Internet "a unique and wholly new medium of worldwide human communication."

The Internet's perceived novelty has prompted regulators to engage in "Internet exceptionalism," crafting Internet-specific laws that diverge from regulatory precedents in other media. Internet exceptionalism has come in three distinct waves:

The First Wave: Internet Utopianism

In the mid-1990s, some people fantasized about an Internet "utopia" that would overcome the problems inherent in other media. Some regulators, fearing disruption of this possible utopia, sought to treat the Internet more favorably than other media.

47 U.S.C. §230 (a law still on the books) is a flagship example of mid-1990s efforts to preserve Internet utopianism. The statute categorically immunizes online providers from liability for publishing most types of third party content. It was enacted (in part) "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation." The statute is clearly exceptionalist because it treats online providers more favorably than offline publishers—even when they publish identical content.

The Second Wave: Internet Paranoia

Later in the 1990s, the regulatory pendulum swung in the other direction. Regulators still embraced Internet exceptionalism, but instead of favoring the Internet, regulators treated the Internet more harshly than analogous offline activity.

For example, in 2005, a Texas website called Live-shot.com announced that it would offer "Internet hunting." The website allowed paying customers to control, via the Internet, a gun on its game farm. An employee manually monitored the gun and could override the customer's instructions. The website wanted to give people who could not otherwise hunt, such as paraplegics, the opportunity to enjoy the hunting experience.

The regulatory reaction to Internet hunting was swift and severe. Over 3 dozen states banned Internet hunting. California also banned Internet fishing for good measure. However, regulators never explained how Internet hunting is more objectionable than physical space hunting.

For example, California Sen. Debra Bowen criticized Internet hunting because it "isn't hunting; it's an inhumane, over the top, pay-per-view video game using live animals for target practice….Shooting live animals over the Internet takes absolutely zero hunting skills, and it ought to be offensive to every legitimate hunter."

Sen. Bowen's remarks reflect numerous unexpressed assumptions about the nature of "hunting" and what constitutes fair play. In the end, however, hunting may just be "hunting," in which case the response to Internet hunting may just be a typical example of adverse Internet exceptionalism.

The Third Wave: Exceptionalism Proliferation

The past few years have brought a new regulatory trend. Regulators are still engaged in Internet exceptionalism, but each new advance in Internet technology has prompted exceptionalist regulations towards that technology.

For example, the emergence of blogs and virtual worlds has helped initiate a push towards blog-specific and virtual world-specific regulation. In effect, Internet exceptionalism has splintered into pockets of smaller exceptionalist efforts.

Regulatory responses to social networking sites like Facebook and MySpace are a prime example of Internet exceptionalism splintering. Rather than regulating these sites like other websites, regulators have sought social networking site-specific laws, such as requirements to verify users' age, combat sexual predators and suppress content that promotes violence. The result is that the regulation of social networking sites differs not only from offline enterprises but from other websites as well.

Implications

Internet exceptionalism is not inherently bad. In some cases, the Internet truly is unique, special or different and should be regulated accordingly. Unfortunately, more typically, exceptionalism cannot be analytically justified and instead reflects regulatory panic.

In these cases, regulatory exceptionalism can be harmful, especially to Internet entrepreneurs and their investors. It can distort the marketplace between web enterprises and their offline competition—occasionally advantaging the website (such as 47 USC 230), but typically hindering the web business' ability to compete. In extreme cases, such as Internet hunting, unjustified regulatory intervention may put companies out of business.

Accordingly, before enacting exceptionalist Internet regulation, regulators should articulate how the Internet is unique, special or different and explain why these differences support exceptionalism. Unfortunately, emotional overreactions to perceived Internet threats or harms typically trump such a rational regulatory process. Knowing this tendency, perhaps we can better resist that temptation.

Doe v. MySpace, Inc., 528 F.3d 413 (5th Cir. 2008).
Clement, Circuit Judge.

Jane and Julie Doe ("the Does") appeal the district court's dismissal of their claims for negligence and gross negligence, and its finding that the claims were barred by the Communications Decency Act ("CDA"), 47 U.S.C § 230, and Texas common law. For the following reasons, we affirm the decision of the district court.

I. FACTS AND PROCEEDINGS

MySpace.com is a Web-based social network. Online social networking is the practice of using a Web site or other interactive computer service to expand one's business or social network. Social networking on MySpace.com begins with a member's creation of an online profile that serves as a medium for personal expression, and can contain such items as photographs, videos, and other information about the member that he or she chooses to share with other MySpace.com users. Members have complete discretion regarding the amount and type of information that is included in a personal profile. Members over the age of sixteen can choose the degree of privacy they desire regarding their profile; that is, they determine who among the MySpace.com membership is allowed to view their profile. Once a profile has been created, the member can use it to extend "invitations" to existing friends who are also MySpace.com users and to communicate with those friends online by linking to their profiles, or using e-mail, instant messaging, and blogs, all of which are hosted through the MySpace.com platform.

Members can also meet new people at MySpace.com through user groups focused on common interests such as film, travel, music, or politics. MySpace.com has a browser feature that allows members to search the Web site's membership using criteria such as geographic location or specific interests. MySpace.com members can also become online "friends" with celebrities, musicians, or politicians who have created MySpace.com profiles to publicize their work and to interface with fans and supporters.

MySpace.com membership is free to all who agree to the Terms of Use. To establish a profile, users must represent that they are at least fourteen years of age. The profiles of members who are aged fourteen and fifteen are automatically set to "private" by default, in order to limit the amount of personal information that can be seen on the member's profile by MySpace.com users who are not in their existing friends network and to prevent younger teens from being contacted by users they do not know. Although MySpace.com employs a computer program designed to search for clues that underage members have lied about their age to create a profile on the Web site, no current technology is foolproof. All members are cautioned regarding the type of information they release to other users on the Web site, including a specific prohibition against posting personal information such as telephone numbers, street addresses, last names, or e-mail addresses. MySpace.com members are also encouraged to report inaccurate, inappropriate, or obscene material to the Web site's administrators.

In the summer of 2005, at age thirteen, Julie Doe ("Julie") lied about her age, represented that she was eighteen years old, and created a profile on MySpace.com. This action allowed her to circumvent all safety features of the Web site and resulted in her profile being made public;

nineteen-year-old Pete Solis ("Solis") was able to initiate contact with Julie in April 2006 when she was fourteen. The two communicated offline on several occasions after Julie provided her telephone number. They met in person in May 2006, and, at this meeting, Solis sexually assaulted Julie.[2]…

III. DISCUSSION

In October 1998[*], Congress recognized the rapid development of the Internet and the benefits generated by Web-based service providers to the public. In light of its findings, Congress enacted the CDA for several policy reasons, including "to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material." To achieve that policy goal, Congress provided broad immunity under the CDA to Web-based service providers for all claims stemming from their publication of information created by third parties, referred to as the "Good Samaritan" provision. Indeed, "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section."

Courts have construed the immunity provisions in § 230 broadly in all cases arising from the publication of user-generated content. For example, the Ninth Circuit held that a Web-based dating-service provider was not liable when an unidentified party posted a false online personal profile for a popular actress, causing her to receive sexually explicit phone calls, letters, and faxes at her home. Acknowledging that the immunity provision in § 230(c)(1) of the CDA causes "Internet publishers [to be] treated differently from corresponding publishers in print, television and radio," the Ninth Circuit held that "[u]nder § 230(c), ... so long as a third party willingly provides the essential published content, the interactive service provider receives full immunity regardless of the specific editing or selection process."

Similarly, the Fourth Circuit dismissed a plaintiff's claims on the pleadings, holding that the CDA protects Web-based service providers from liability even after the provider is notified of objectionable content on its site. The plaintiff in *Zeran* sued an Internet service provider for failing to remove upon notice a false advertisement offering shirts featuring tasteless slogans relating to the 1995 bombing of the Oklahoma City Federal Building and instructing interested buyers to call the plaintiff to place orders. After analyzing the immunity provision of § 230, the Fourth Circuit wrote:

> If computer service providers were subject to distributor liability, they would face potential liability each time they receive notice of a potentially defamatory statement-from any party, concerning any message.... Because service providers would be subject to liability only for the publication of information, and not for its removal, they would have a natural incentive simply to remove messages upon notification, whether the contents were defamatory or not. Thus, like strict liability, liability upon notice has a chilling effect on the freedom of Internet

[2] Julie's mother reported the assault to Austin, Texas police, who arrested Solis and charged him with second-degree sexual assault.

[*] [Ed. note: this date appears to be an error. The DMCA was enacted in October 1998. The CDA was enacted in February 1996.]

> speech.... Because the probable effects of distributor liability on the vigor of Internet speech and on service provider self-regulation are directly contrary to § 230's statutory purposes, we will not assume that Congress intended to leave liability upon notice intact.

Parties complaining that they were harmed by a Web site's publication of user-generated content have recourse; they may sue the third-party user who generated the content, but not the interactive computer service that enabled them to publish the content online.

The Does appear to agree with the consensus among courts regarding the liability provisions in § 230(c)(1). They argue, however, that their claims against MySpace do not attempt to treat it as a "publisher" of information; therefore, they argue that § 230 does not immunize MySpace from their claims and state tort law applies in full effect. The Does attempt to distinguish their case from *Carafano*, *Zeran*, and other contrary authority by claiming that this case is predicated solely on MySpace's failure to implement basic safety measures to protect minors. The district court rejected the Does' argument, stating:

> The Court, however, finds this artful pleading to be disingenuous. It is quite obvious the underlying basis of Plaintiffs' claims is that, through postings on MySpace, Pete Solis and Julie Doe met and exchanged personal information which eventually led to an in-person meeting and the sexual assault of Julie Doe. If MySpace had not published communications between Julie Doe and Solis, including personal contact information, Plaintiffs assert they never would have met and the sexual assault never would have occurred. No matter how artfully Plaintiffs seek to plead their claims, the Court views Plaintiffs' claims as directed toward MySpace in its publishing, editorial, and/or screening capacities.

The Does do not present any caselaw to support their argument. In fact, they rely upon the same line of cases listed above but point to § 230(c)(1)'s grant of immunity to publishers of third-party content as evidence that their claims are somehow different. Other courts, however, have examined pleadings similar to the Does' and have reached the same conclusion as the district court. For example, in *Green*, the plaintiff sued a Web-based service provider after he received a computer virus from a third party and endured derogatory comments directed at him by others in an online "chat room." He made a failure-to-protect argument similar to the Does', claiming that "AOL waived its immunity under [§] 230 by the terms of its membership contract with him and because AOL's Community Guidelines outline standards for online speech and conduct and contain promises that AOL would protect [him] from other subscribers." The Third Circuit, however, dismissed the claims as barred by § 230, after recharacterizing the plaintiff's claims:

> There is no real dispute that Green's fundamental tort claim is that AOL was negligent in promulgating harmful content and in failing to address certain harmful content on its network. Green thus attempts to hold AOL liable for decisions relating to the monitoring, screening, and deletion of content from its network-actions quintessentially related to a publisher's role. Section 230 "specifically proscribes liability" in such circumstances.

Green demonstrates the fallacy of the Does' argument. Their claims are barred by the CDA, notwithstanding their assertion that they only seek to hold MySpace liable for its failure to implement measures that would have prevented Julie Doe from communicating with Solis. Their allegations are merely another way of claiming that MySpace was liable for publishing the communications and they speak to MySpace's role as a publisher of online third-party-generated content.

The Does further argue for the first time on appeal that MySpace is not immune under the CDA because it partially created the content at issue, alleging that it facilitates its members' creation of personal profiles and chooses the information they will share with the public through an online questionnaire. The Does also contend that MySpace's search features qualify it as an "information content provider", as defined in the CDA: "The term 'information content provider' means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service."

Nothing in the record, however, supports such a claim; indeed, Julie admitted that she lied about her age to create the profile and exchanged personal information with Solis. In the February 1, 2007 hearing before the district court, the Does admitted that Julie created the content, disclosing personal information that ultimately led to the sexual assault, but stressed that their cause of action was rooted in the fact that MySpace should have implemented safety technologies to prevent Julie and her attacker from meeting:

> THE COURT: I want to get this straight. You have a 13-year-old girl who lies, disobeys all of the instructions, later on disobeys the warning not to give personal information, obviously, [and] does not communicate with the parent. More important, the parent does not exercise the parental control over the minor. The minor gets sexually abused, and you want somebody else to pay for it? This is the lawsuit that you filed?
>
> MR. ITKIN [Counsel for the Does]: Yes, your Honor.
>
> ....
>
> MR. ITKIN: The first point is we're not complaining about any of the content that was transmitted between Julie Doe and Pete Solis. Our complaint is [that] the two of them never should have been able to meet because MySpace could have implemented technology very simple and technologically-not simple but technologically and inexpensive age verification software that has been asked for by attorneys general before the lawsuit happened, or even done the things they did right after the filing of the lawsuit that would have prevented these two people from ever meeting. We wanted to keep the foxes out of the hen house. That's the first thing, your Honor, is that we're not complaining about the content.

Throughout the hearing, the Does stated they had one argument—that MySpace was negligent for not taking more precautions:

> MR. ITKIN: Pete Solis is liable for an assault. But what we're trying to hold MySpace liable for isn't the publishing of a phone number but, rather, we're trying to hold MySpace responsible for not putting in the safety precautions to keep the two of them separated.
>
> ....
>
> THE COURT: Now, I've heard all of your arguments on the negligence and the duty. Now the duty is something that's bothering me and that's my next question to you. But as I read your pleadings, they are just wholly inapplicable to the Federal Rules of Procedure on fraud. You've got no specific fraud here. And on your negligent misrepresentation, that's just a rehash of what you're already doing. So we're really talking about one cause of action, and that is a negligence cause of action. You keep nodding. Do you agree with that?
>
> MR. ITKIN: I think that is a fair recommendation, a fair statement.
>
> ....
>
> MR. ITKIN: Thank you. Your Honor we are not—and I want to be very clear about this. We are not complaining about any of the content that was exchanged between Julie Doe and Pete Solis. We understand that that is something we cannot complain about. Our complaint is only that these two should have never been allowed to find each other, anyways, if reasonable safety precautions were put in place. And under congressional law and, we believe, Texas common law, that's enough to state a claim.

Although the Does' complaint alleged that MySpace allowed or encouraged members to post information *after* a member's profile had been created, counsel for the Does reiterated in the hearing time and again that they had no complaints or allegations regarding the content of the information posted by Julie or exchanged between Julie and Solis. It appears that the reference to MySpace's solicitation of information was solely used to set up the Does' argument that MySpace failed to protect Julie by declining to implement age-verification software:

> THE COURT: But your client violated every single thing that MySpace says to do.
>
> MR. ITKIN: Which is your Honor—and true. That is correct, your Honor. But I will say that that's a known risk to MySpace. And that's not just me saying it, that's the Attorney General saying it.
>
> THE COURT: Everyone knows people lie. So therefore, should you be liable?

> MR. ITKIN: No, your Honor. But when you know of the risk and you know that the people-there's potential for lying, all you need to do is put some basic safety mechanisms in place to prevent—or to circumvent the lying.
>
> THE COURT: So you've got the Attorney General of the United States saying ... don't put your credit card on the internet, but you want them to do it to get a free space. That's one of the things.
>
> MR. ITKIN: That's one of the things.
>
> THE COURT: Then a driver's license. Do you know how many people I sentence here every Friday that have a fake driver's license?
>
> MR. ITKIN: I can imagine a lot, your Honor.
>
> ....
>
> MR. ITKIN: What we really want, your Honor, is there's a company out there—I'll give you an example of one of the companies out there called Aristotle. Aristotle through public databases if you enter your name, your zip code, and your birth year can come back with, hey, this person's real; or you can enter an e-mail and have verification. So there's some things to do that are less intrusive as far as giving people your driver's license or your Social Security number.
>
> ....
>
> MR. ITKIN: Your Honor, because if [MySpace] had the age verification software in place, [Julie and Solis] never would have talked in the first place. They never would have known about each other.

At no time before filing their appeal in this Court did the Does argue that the CDA should not apply to MySpace because it was partially responsible for creating information exchanged between Julie and Solis. Because the Does failed to present this argument to the district court, they are barred from making this argument on appeal. We therefore hold, without considering the Does' content-creation argument, that their negligence and gross negligence claims are barred by the CDA, which prohibits claims against Web-based interactive computer services based on their publication of third-party content. Because we affirm the district court based upon the application of § 230(c)(1), there is no need to apply § 230(c)(2), or to assess the viability of the Does' claims under Texas common law in the absence of the CDA….

Moreno v. Hanford Sentinel, Inc., 172 Cal. App. 4th 1125 (Cal. App. Ct. 2009).
Levy, Judge.

The issue presented by this appeal is whether an author who posts an article on myspace.com can state a cause of action for invasion of privacy and/or intentional infliction of emotional distress against a person who submits that article to a newspaper for republication. The trial court concluded not and sustained the demurrer to appellants' complaint without leave to amend.

Appellants contend the republication constituted a public disclosure of private facts that were not of legitimate public concern and thus was an invasion of privacy. Appellants note that the republication included the author's last name whereas the myspace.com posting did not. Appellants further argue that the person who submitted the article to the newspaper did so with the intent of punishing appellants and thus they have a claim for intentional infliction of emotional distress.

As discussed in the published portion of this opinion, the trial court properly sustained the demurrer without leave to amend to appellants' invasion of privacy cause of action. The facts contained in the article were not private. Rather, once posted on myspace.com, this article was available to anyone with internet access. As discussed in the nonpublished portion, the trial court should have overruled the demurrer to the intentional infliction of emotional distress cause of action. Under the circumstances here, a jury should determine whether the alleged conduct was outrageous. Accordingly, the judgment will be affirmed in part and reversed in part.

BACKGROUND…

Following a visit to her hometown of Coalinga, appellant, Cynthia Moreno, wrote "An ode to Coalinga" (Ode) and posted it in her online journal on myspace.com. The Ode opens with "the older I get, the more I realize how much I despise Coalinga" and then proceeds to make a number of extremely negative comments about Coalinga and its inhabitants. Six days later, Cynthia removed the Ode from her journal. At the time, Cynthia was attending the University of California at Berkeley. However, Cynthia's parents, appellants David and Maria Moreno, and Cynthia's sister, appellant Araceli Moreno, were living in Coalinga. Araceli was a student at Coalinga High School.

Respondent, Roger Campbell, was the principal of Coalinga High School and an employee of respondent, Coalinga-Huron Unified School District. The day after Cynthia removed the Ode from her online journal, appellants learned that Campbell had submitted the Ode to the local newspaper, the Coalinga Record, by giving the Ode to his friend, Pamela Pond. Pond was the editor of the Coalinga Record.

The Ode was published in the Letters to the Editor section of the Coalinga Record. The Ode was attributed to Cynthia, using her full name. Cynthia had not stated her last name in her online journal.

The community reacted violently to the publication of the Ode. Appellants received death threats and a shot was fired at the family home, forcing the family to move out of Coalinga. Due to

severe losses, David closed the 20-year-old family business.

Based on the publication of the Ode, appellants filed the underlying complaint alleging causes of action for invasion of privacy and intentional infliction of emotional distress. In addition to respondents, appellants named Lee Enterprises, Inc., Lee Enterprises Newspapers, Inc., and Hanford Sentinel, Inc., the publishers of the Coalinga Record, as defendants. However, these publisher defendants were dismissed following their motion to strike the complaint as a SLAPP suit (strategic lawsuits against public participation) pursuant to Code of Civil Procedure section 425.16. Appellants abandoned their appeal from this judgment.

DISCUSSION

1. Appellants did not state a cause of action for invasion of privacy.

The right to privacy tort was recognized in 1890 based on the trend in tort law to extend protection to "'the right of determining, ordinarily, to what extent [a person's] thoughts, sentiments, and emotions shall be communicated to others.'" In other words, the tort protects "a 'right "to be let alone."'" In 1972, the right to privacy was added to the California Constitution by initiative.

To state a claim for violation of the constitutional right of privacy, a party must establish (1) a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; and (3) a serious invasion of the privacy interest. Four distinct kinds of activities have been found to violate this privacy protection and give rise to tort liability. These activities are: (1) intrusion into private matters; (2) public disclosure of private facts; (3) publicity placing a person in a false light; and (4) misappropriation of a person's name or likeness. Each of these four categories identifies a distinct interest associated with an individual's control of the process or products of his or her personal life. However, to prevail on an invasion of privacy claim, the plaintiff must have conducted himself or herself in a manner consistent with an actual expectation of privacy.

Here, the allegations involve a public disclosure of private facts. The elements of this tort are: "'(1) public disclosure (2) of a private fact (3) which would be offensive and objectionable to the reasonable person and (4) which is not of legitimate public concern.'" The absence of any one of these elements is a complete bar to liability.

a. Having been published on myspace.com, the Ode was not private.
As noted above, a crucial ingredient of the applicable invasion of privacy cause of action is a public disclosure of *private facts*. A matter that is already public or that has previously become part of the public domain is not private.

Here, Cynthia publicized her opinions about Coalinga by posting the Ode on myspace.com, a hugely popular internet site. Cynthia's affirmative act made her article available to any person with a computer and thus opened it to the public eye. Under these circumstances, no reasonable person would have had an expectation of privacy regarding the published material.

As pointed out by appellants, to be a private fact, the expectation of privacy need not be absolute. Private is not equivalent to secret. "[T]he claim of a right of privacy is not '"so much one of total secrecy as it is of the right to *define* one's circle of intimacy—to choose who shall see beneath the quotidian mask."' Information disclosed to a few people may remain private." Nevertheless, the fact that Cynthia expected a limited audience does not change the above analysis. By posting the article on myspace.com, Cynthia opened the article to the public at large. Her potential audience was vast.

That Cynthia removed the Ode from her online journal after six days is also of no consequence. The publication was not so obscure or transient that it was not accessed by others. The only place that Campbell could have obtained a copy of the Ode was from the internet, either directly or indirectly.

Finally, Cynthia's last name was not a private fact. Although her online journal only used the name "Cynthia," it is clear that her identity was readily ascertainable from her MySpace page. Campbell was able to attribute the article to her from the internet source. There is no allegation that Campbell obtained Cynthia's identification from a private source. In fact, Cynthia's MySpace page included her picture. Thus, Cynthia's identity as the author of the Ode was public. In disclosing Cynthia's last name, Campbell was merely giving further publicity to already public information. Such disclosure does not provide a basis for the tort.

b. The other members of Cynthia's family do not have an independent cause of action for invasion of privacy.

Based on the direct damages they allegedly incurred due to publication of the Ode, Cynthia's parents, David and Maria, and Cynthia's sister, Araceli, argue that they have standing to sue for invasion of privacy. However, because the publication of the Ode was not an invasion of Cynthia's privacy, these appellants cannot state a claim based on the same alleged invasion.

Moreover, the right of privacy is purely personal. It cannot be asserted by anyone other than the person whose privacy has been invaded. Thus, even if Cynthia did have an invasion of privacy claim, David, Maria and Araceli would not have standing. The Coalinga Record did not identify David, Maria and Araceli when it published the Ode. Their invasion of privacy claim is primarily based on their relationship to Cynthia and the community reaction to Cynthia's opinions, not on respondents' conduct directed toward them.

In sum, because the Ode was not private, appellants' claim is precluded under California privacy tort law.[4] Accordingly, the trial court properly sustained the demurrer to the invasion of privacy cause of action.

2. A jury must determine whether respondents' conduct was sufficiently extreme and outrageous to result in liability for intentional infliction of emotional distress.[*]

[4] Whether the publication of the Ode infringed on any federal copyright protection the Ode may have had is not before this court and we express no opinion on that issue.

[*] [Ed. note: this portion of the opinion was not certified for publication.]

"The elements of a cause of action for intentional infliction of emotional distress are (1) outrageous conduct by the defendant, (2) intention to cause or reckless disregard of the probability of causing emotional distress, (3) severe emotional suffering, and (4) actual and proximate causation of the emotional distress."

To be outrageous, conduct must be so extreme that it exceeds all bounds of that usually tolerated in a civilized community. However, conduct that might not otherwise be considered extreme and outrageous may be found to be so if a (1) defendant abuses a relation or position that gives him power to damage the plaintiff's interest; (2) knows the plaintiff is susceptible to injuries through mental distress; or (3) acts intentionally or unreasonably with the recognition that the acts are likely to result in illness through mental distress.

It is for the court to determine in the first instance whether the defendant's conduct may reasonably be regarded as so extreme and outrageous as to permit recovery. In making this determination, the court employs an objective standard applied to the actual conduct, i.e., how reasonable people might view it, excluding from that category those who are either overly sensitive or callous. But, "'[w]here reasonable men may differ, it is for the jury, subject to the control of the court, to determine whether, in the particular case, the conduct has been sufficiently extreme and outrageous to result in liability.'" Here, the trial court concluded that Campbell's conduct did not meet the standard of outrageousness necessary to constitute a cause of action for intentional infliction of emotional distress as a matter of law.

In stating their claim for intentional infliction of emotional distress, appellants alleged that Campbell submitted the Ode to the Coalinga Record, knowing he did not have permission to do so. Appellants further alleged that Campbell engaged in this act to punish appellants for the contents of the Ode and intended to cause them emotional distress. Appellants contend that this conduct was extreme and outrageous, especially in light of Campbell's position as Araceli's principal.

Since this appeal is from the sustaining of a demurrer without leave to amend, this court must assume the truth of appellants' allegations against Campbell. Based on these allegations, we conclude that reasonable people may differ on whether Campbell's actions were extreme and outrageous. Accordingly, it is for a jury to make this determination. Thus, the trial court erred in sustaining the demurrer to the intentional infliction of emotional distress cause of action….